Table of Contents

Health and Safety Precautions **5**
General Use Precautions 5

1. Introduction to the LaCie Ethernet Disk RAID **7**

2. About Your LaCie Ethernet Disk RAID **8**
2.1. Package Content 8
2.2. Minimum System Requirements 9
2.2. Views of the System 10

3. Installing Your LaCie Ethernet Disk RAID **13**
3.1. Connecting the Ethernet Disk RAID to the Network 13
3.2. Turning On the Ethernet Disk RAID 14

4. Configuring Your LaCie Ethernet Disk RAID **15**
4.1. Installing the Ethernet Disk RAID Console 16
4.2. Starting the Console 17
4.3. Initializing the Disks 18
4.4. Configuring with the First Use Wizard 19
4.5. USB Devices 22
4.5.1. Attaching USB Devices 22
4.5.2. Disconnecting USB Devices 22

5. Managing Your LaCie Ethernet Disk RAID **23**
5.1. Accessing the Manager 24
5.2. Logging In to the Manager 24
5.3. Navigating the Manager 25
5.3.1. Storage Status Tab 26
5.3.2. Connection Status Tab 26
5.4. Managing Users 27
5.4.1. Adding Users 27
5.4.2. Modifying Users 30
5.4.3. Removing Users 31
5.4.4. Working with Groups 32
5.4.4.1. Adding a Group 32
5.4.4.2. Changing the Group Membership 34
5.4.4.3. Removing a Group 35
5.5. Managing Shared Folders 36
5.5.1. Creating Shared Folders 36
5.5.2. Changing User Access to Shared Folders 39
5.5.3. Deleting a Shared Folder 41
5.6. Managing Backups 42

5.6.1. Changing the Recovery Password 42
5.6.2. Configuring Remote Boot 43
5.6.3. Deleting a Backup 44
5.6.4. Deleting a Client 45
5.7. Advanced Management 46
5.7.1. Alerts 46
5.7.2. Firmware 48
5.7.3. USB 49
5.7.4. System 50
5.7.5. Network 52
5.7.6. Reconfiguring the Disks 56
5.7.6.1. Expanding the Shared Storage 57
5.7.6.2. Reconfiguring the Disks 58
5.7.7. System Status 60
5.7.8. System Log 61
5.7.9. Shut Down 62
5.8. Logging Out of the Manager 62

6. Working With Shared Folders 63
6.1. Accessing Shared Folders 63
6.1.1. Windows Users 63
6.1.1.1. Using My Computer or Windows Explorer 64
6.1.1.2. Using the Console 65
6.1.2. Linux Users 67
6.1.2.1. Using NFS 67
6.1.2.2. Using SMBFS 68
6.1.3. Mac Users 69
6.1.3.1. Mac OS X 69
6.1.3.2. Other Mac Operating Systems 69
6.2. Accessing Shared Folders Using FTP 70
6.3. Disconnecting from Shared Folders 71
6.3.1. Windows Users 71
6.3.1.1. Using My Computer or Windows Explorer 71
6.3.1.2. Using the Console 71
6.3.2. Linux Users 72
6.3.3. Mac OS X Users 72
6.3.4. Other Mac Users 72

7. Protecting Local Disks 73
7.1. Getting Started 74
7.1.1. System Requirements 74
7.1.2. Additional Requirements 75
7.1.3. Installing the Microsoft iSCSI Initiator 75
7.1.4. Installing Windows Backup Software 76

7.1.5. Starting Windows Backup Software 80
7.1.6. Activating Your License 81
7.1.7. Activating Your License with an Internet Connection 82
7.1.8. Replacing Your Existing License 82
7.2. Protecting Your Disks 83
7.3. Manually Backing Up Your Disk 89
7.4. Stopping a Backup or Recovery in Progress 90
7.5. Changing the Backup Schedule 91
7.6. Receiving Event Notifications 92
7.7. Changing the Recovery Password 93
7.8. Enabling or Disabling Remote Boot 94
7.8.1. Enabling Remote Boot 95
7.8.2. Disabling Remote Boot 96
7.9. Recovering Data 97
7.9.1. Recovering Files or Folders 98
7.9.2. Recovering a Data Disk 100
7.9.3. Recovering a System Disk Using the Recovery CD 102
7.9.4. Recovering a System Disk Using While Booting Remotely 108
7.9.5. Removing Protection 112

8. Troubleshooting 113
8.1. Troubleshooting the Ethernet Disk RAID 113
8.2. Troubleshooting Windows Backup Software 116
8.3. Creating a Diagnostic File 118
8.3.1. Using Windows Backup Software 118
8.3.2. Using the Recovery CD 118
8.4. Resetting the Recovery Password in the Microsoft iSCSI Initiator 119

9. Technical Specifications 120
9.1. Hardware Specification 120
9.2. Software Specification 121

10. Understanding RAID and Storage Policies 122
10.1. RAID 0 123
10.2. RAID 1 124
10.3. RAID 5 125
10.4. RAID 5 + Spare 126
10.5. RAID 10 (RAID 1 + 0) 127

11. Contacting Customer Support 128
11.1. LaCie Technical Support Contacts 129

12. Warranty Information 130

Glossary 131

Copyrights

Copyright © 2006 LaCie. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of LaCie.

Trademarks

Apple, Mac, and Macintosh are registered trademarks of Apple Computer, Inc. Microsoft, Windows 98, Windows 98 SE, Windows 2000, Windows Millennium Edition and Windows XP are registered trademarks of Microsoft Corporation. Other trademarks mentioned in this manual are the property of their respective owners.

Changes

The material in this document is for information only and subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, LaCie assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. LaCie reserves the right to make changes or revisions in the product design or the product manual without reservation and without obligation to notify any person of such revisions and changes.

LaCie Ethernet Disk
RAID Storage System
Tested To Comply
With FCC standards
For Home or Office Use

Canada Compliance Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

1. The devices may not cause harmful interference
2. The devices must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by LaCie could void the FCC & Industry Canada regulations and negate your authority to operate the product.

CAUTION: Modifications not authorized by the manufacturer may void the user's authority to operate this device.

Manufacturer's Declaration for CE Certification

We, LaCie, solemnly declare that this product conforms to the following European standards: Class B EN60950, EN55022, EN55024

With reference to the following conditions: 73/23/EEC Low Voltage Directive; 89/336/EEC EMC Directive

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designed collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service, or the shop where you purchased the product.

CAUTION: The LaCie Ethernet Disk RAID warranty may be void as a result of the failure to respect the precautions listed above.

Health and Safety Precautions

Only qualified persons are authorized to carry out maintenance on this device.

Read this User Manual carefully and follow the correct procedure when setting up the device.

- The power button DOES NOT turn off the system AC power. To remove power from the Ethernet Disk RAID, you must unplug the AC power cord from the wall outlet or the chassis.
- Read this User's Guide carefully, and follow the correct procedure when setting up the device.
- Do not open your LaCie Ethernet Disk RAID or attempt to disassemble or modify it. Never insert any metallic object into the drive to avoid any risk of electrical shock, fire, short-circuiting or dangerous emissions. Your LaCie Ethernet Disk RAID contains no user-serviceable parts. If it appears to be malfunctioning, have it inspected by a qualified LaCie Technical Support representative.
- Never expose your device to rain, or use it near water, or in damp or wet conditions. Never place objects containing liquids on the LaCie Ethernet Disk RAID, as they may spill into its openings. Doing so increases the risk of electrical shock, short-circuiting, fire or personal injury.
- Make sure that the computer and LaCie Ethernet Disk RAID are electrically grounded. If the devices are not grounded, there is an increased risk of electrical shock. Power requirements 100-240 V~, 4-2 A, 60-50 Hz, (Supply voltage fluctuations not exceeding ± 10% of the nominal, transient over-voltages according to over-voltage category II).

General Use Precautions

- Do not expose the LaCie Ethernet Disk RAID to temperatures outside the range of 5° C to 35° C (41° F to 95° F); or to operational humidity beyond 5-80%, non-condensing, or non-operating humidity beyond 10-90%, non-condensing. Doing so may damage the LaCie Ethernet Disk RAID or disfigure its casing. Avoid placing your LaCie Ethernet Disk RAID near a source of heat or exposing it to sunlight (even through a window). Inversely, placing your LaCie Ethernet Disk RAID in an environment that is too cold or humid may damage the unit.
- Always unplug the LaCie Ethernet Disk RAID from the electrical outlet if there is a risk of lightning or if it will be unused for an extended

period of time. Otherwise, there is an increased risk of electrical shock, short-circuiting or fire.

- Do not use the LaCie Ethernet Disk RAID near other electrical appliances such as televisions or radios. Doing so may cause interference which will adversely affect the operation of the other products.
- Do not place the LaCie Ethernet Disk RAID near sources of magnetic interference, such as computer displays, televisions or speakers. Magnetic interference can affect the operation and stability of your LaCie Ethernet Disk RAID.
- Do not place heavy objects on top of the LaCie Ethernet Disk RAID or use excessive force on it.

Never use excessive force on your LaCie Ethernet Disk RAID. If you detect a problem, see the Troubleshooting section in this manual.

CAUTION: A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.

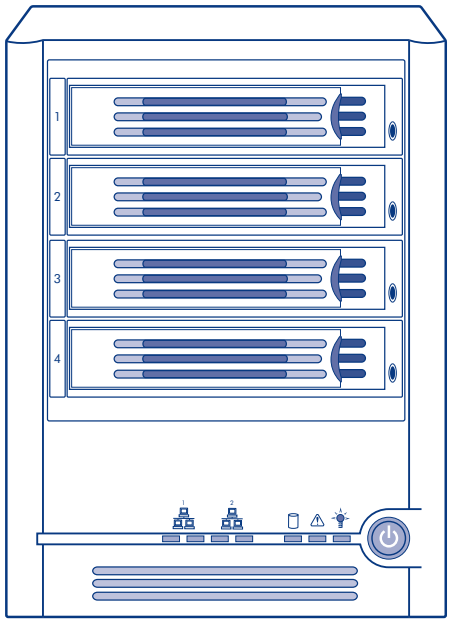
IMPORTANT INFO: 1GB = 1,000,000,000 bytes. 1TB = 1,000,000,000,000 bytes. Once formatted, the actual available storage capacity varies depending on operating environment (typically 5-10% less). In addition, the amount of used backup capacity will be greater than the total size of all the disks listed on the Backups page because additional storage space is needed for the data that has changed between backups. Actual capacity depends on RAID level (see page 117).

IMPORTANT INFO: Any loss, corruption or destruction of data while using a LaCie drive is the sole responsibility of the user, and under no circumstances will LaCie be held liable for the recovery or restoration of this data. To help prevent the loss of your data, LaCie highly recommends that you keep TWO copies of your data; one copy on your external hard drive, for instance, and a second copy either on your internal hard drive, another external hard drive or some other form of removable storage media. LaCie offers a complete line of CD and DVD drives. If you would like more information on backup, please refer to our web site.

1. Introduction to the LaCie Ethernet Disk RAID

The LaCie Ethernet Disk RAID is an intelligent network storage solution for small and medium-sized offices and home network environments. It provides hard disk space for both shared files and backups of your computer hard disks, offering an ideal way to distribute and protect important data.

The Ethernet Disk RAID features an integrated file server with system backup, and ability to manage shared folders by user names or groups. It can connect to a gigabit Ethernet network and support up to four serial ATA (SATA) hard drives. The Ethernet Disk RAID's good performance is ideal for protecting valuable company data, as well as quickly restoring files from a backup.



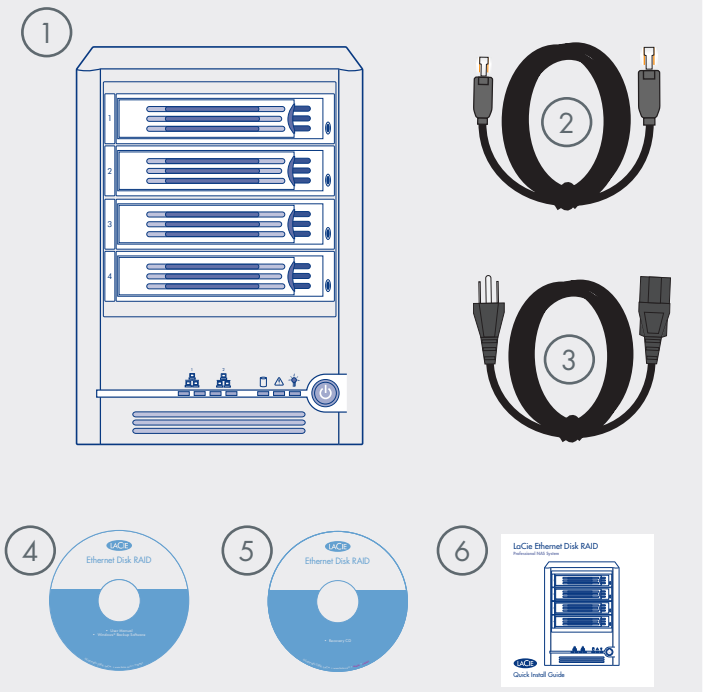
Your LaCie Ethernet Disk RAID Capabilities

- Share huge amounts of data over gigabit ethernet
- Fast backup with SATA connectivity
- Create your own local network

2. About Your LaCie Ethernet Disk RAID

2.1. Package Content

1. LaCie Ethernet Disk RAID tower with 4 removable drive trays and hard drives
2. Ethernet cable
3. Power supply cable
4. LaCie Ethernet Disk RAID Utilities CD-ROM (includes Windows Backup Software, User Manual and Quick Install Guide)
5. LaCie Ethernet Disk RAID Restore CD
6. LaCie Ethernet Disk RAID Quick Install Guide (printed version)



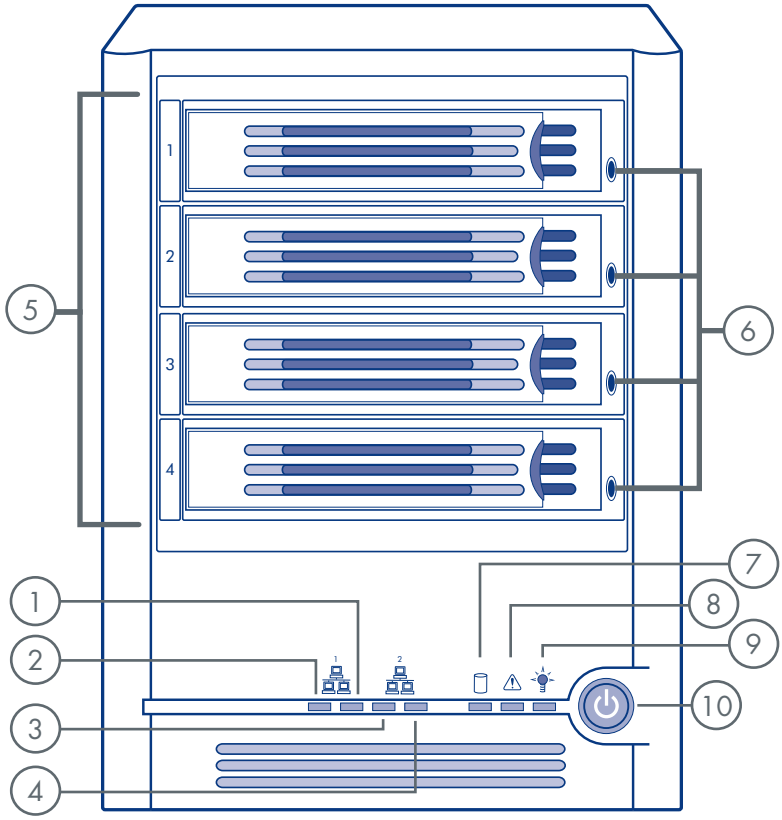
2.2. Minimum System Requirements

Component	Requirement
Web Browser	Microsoft Internet Explorer 6.0 or above, Firefox 1.06 or above
Network Environment	TCP/IP networking environment.
Operating Systems for Folder Access	Microsoft Windows Server 2003, Microsoft Windows 2000 Professional, Microsoft Windows XP Home or Professional, Apple OS X, Linux-based distributions

TECHNICAL NOTE: Macintosh and Linux users can access the network storage device, but Windows is necessary for setup and administration of the device.

2.2. Views of the System

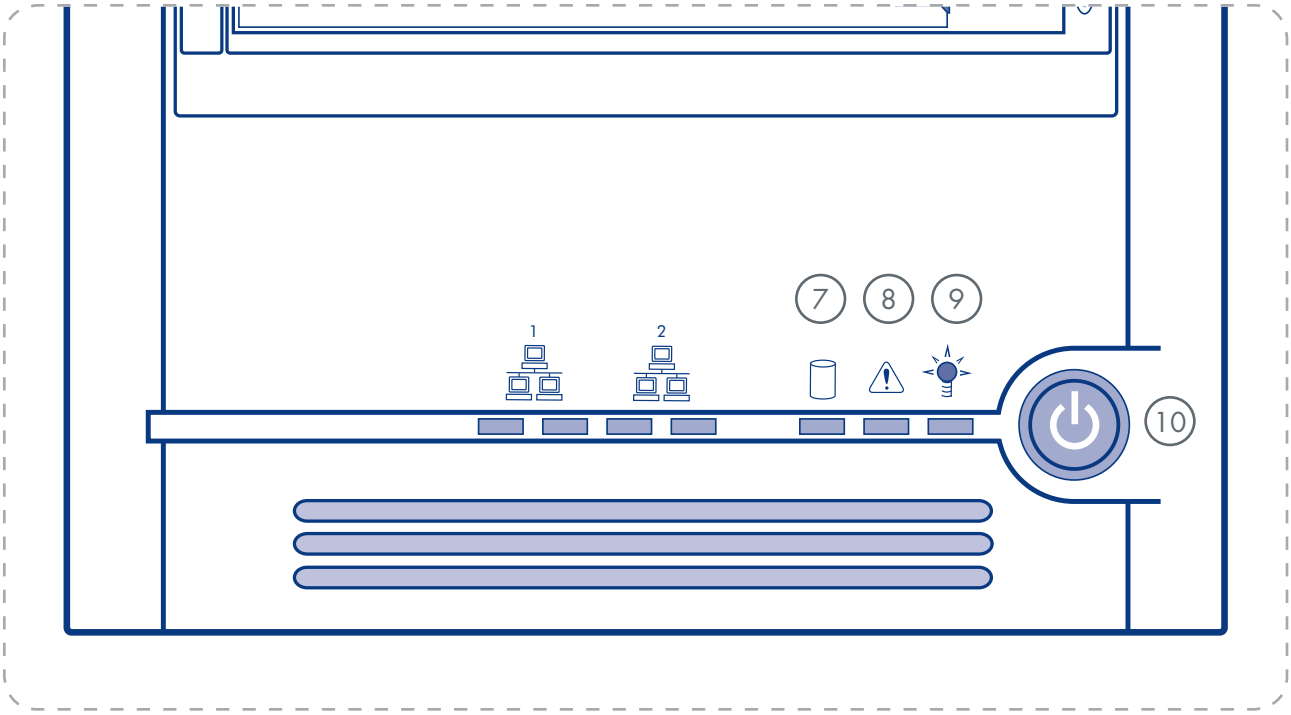
■ Front View



1. **Network Connection 1 Activity LED**– Blinking green indicates Ethernet activity.
2. **Network Connection 1 Link LED** – Continuous GREEN indicates an active Ethernet connection. Off indicates no active Ethernet connection.
3. **Network Connection 2 Link LED** – Blinking green indicates Ethernet activity.
4. **Network Connection 2 Activity LED** – Continuous GREEN indicates an active Ethernet connection. Off indicates no active Ethernet connection.
5. **Drive Carriers 1-4** – 3.5-in. SATA drive carriers
6. **Hard Disk Activity LEDs** –
   - Continuous GREEN indicates the drive is available.
   - Blinking GREEN indicates drive activity.
   - Continuous YELLOW indicates a fault condition, possibly requiring the hard disk to be replaced.
   - Blinking YELLOW indicates the drive is currently rebuilding RAID.

■ (continued, next page)

Front View (continued)



7 **Global Disk Status LED –**

- Continuous GREEN indicates hard disk health is good (1-4 hard disks).
- Continuous YELLOW indicates a critical or non-recoverable condition exists. It also indicates the hard drives are not configured when initially setting up the system.
- Blinking YELLOW indicates (1) one or more hard disks are experiencing a fault condition or (2) a RAID is being rebuilt.

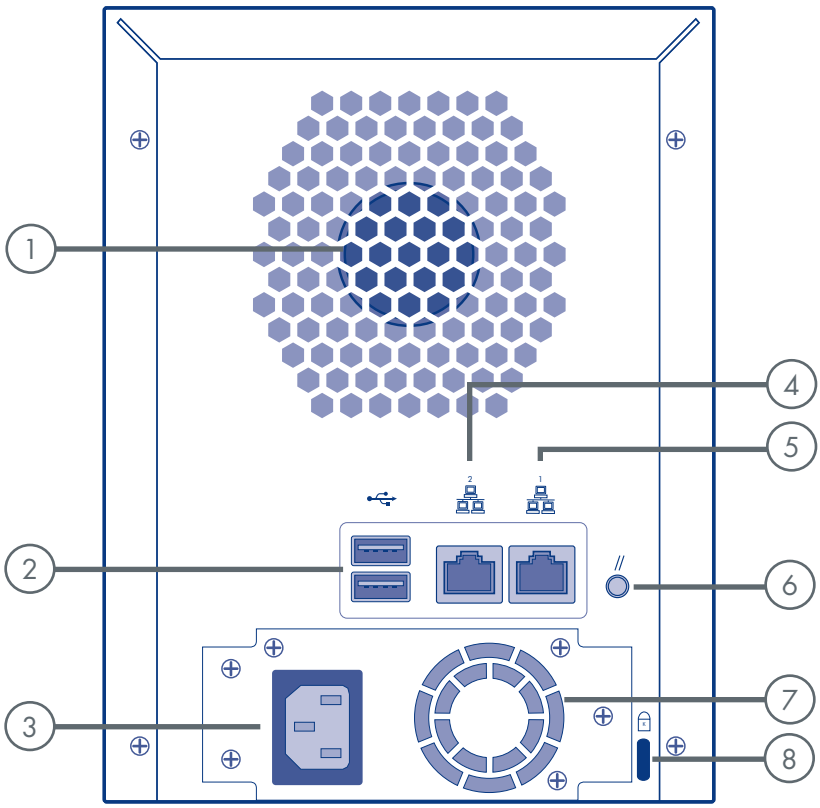
8 **System Status LED –**

- Continuous GREEN indicates the system is running and operating normally.
- Blinking GREEN indicates the system is in process of powering up or shutting down.
- Continuous YELLOW indicates a fault is present, either a critical or non-recoverable condition.

9 **Power LED –** Continuous GREEN indicates the system has power applied to it. No light indicates the system does not have power applied to it.

10 **Power Button –** Toggles the system power on/off.

Rear View



1. **System Fan**
2. **USB 2.0 Ports** – The USB ports are used for connecting an external USB storage device, or for connecting a printer for printer sharing.
3. **Power Connector** – Supplies power to the device.
4. **Gigabit LAN Port 2** – Gigabit Ethernet connection. The right LED lights up GREEN when connected to a 10/100 MB network, and ORANGE when connected to a gigabit network.
5. **Gigabit LAN Port 1** – Gigabit Ethernet connection. The right LED lights up GREEN when connected to a 10/100 MB network, and ORANGE when connected to a gigabit network.
6. **Reset Button** – Press the Reset Button for three seconds to revert the unit to the system defaults.
7. **Power Supply Fan**
8. **Security Slot** – Anti-theft slot for attaching a security cable.

3. Installing Your LaCie Ethernet Disk RAID

Installation of the LaCie Ethernet Disk RAID is easy, just follow the steps below to install it:

Step 1	Connecting the Ethernet Disk RAID to the network	Page 13
Step 2	Turning on the Ethernet Disk RAID	Page 14

3.1. Connecting the Ethernet Disk RAID to the Network

To connect the Ethernet Disk RAID to your network, insert one end of the RJ-45 Ethernet cable into the Ethernet port 1 on the back of the unit (see A in Fig. 3.1.). Then insert the other end of the RJ-45 Ethernet cable into a network port.

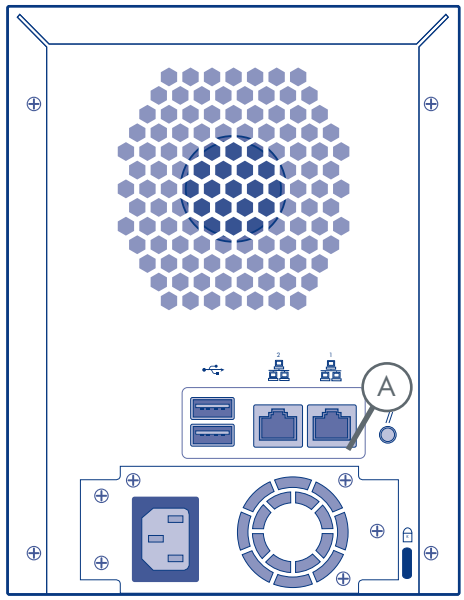


Fig. 3.1.

3.2. Turning On the Ethernet Disk RAID

1. Insert the power cable into the power outlet on the back of the unit and plug the other end into a power socket.
2. Once you have connected the power cord, press the power button on the front (see (A) in Fig. 3.2.).

The System Status LED light will blink green while the Ethernet Disk RAID is booting up. When the system has finished booting up, the System Status LED and Disk Status LED will remain green.

The System Status LED will turn solid yellow when you power up the system for the first time, indicating the hard drives are not configured with a RAID level. It will remain yellow until the drives are configured then the Status System LED will turn solid green.

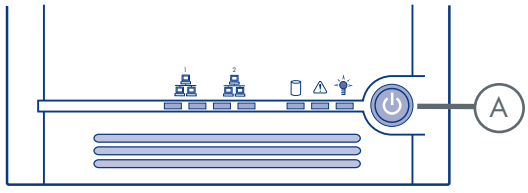


Fig. 3.2.

TECHNICAL NOTE: It is recommended that you plug the Ethernet Disk RAID into a surge protector or uninterruptible power supply to prevent damage to the system from power surges.

4. Configuring Your LaCie Ethernet Disk RAID

Follow the steps below to configure your Ethernet Disk RAID:

Step 1	Installing the Ethernet Disk RAID Console	Page 16
Step 2	Starting the Console	Page 17
Step 3	Initializing the disks	Page 18
Step 4	Configuring with the First Use Wizard	Page 19
Step 10	Attaching USB Devices	Page 22

4.1. Installing the Ethernet Disk RAID Console

To install the console:

1. At a computer in the same subnet as your Ethernet Disk RAID, insert the installation CD into a CD-ROM drive.
2. Your default browser will open a LaCie Ethernet Disk RAID page. Select **Applications** from the top menu.
3. Select the "**Storage System Console**" link to install the software.
4. Follow the Installation Wizard to complete installation of the Console.

TECHNICAL NOTE: To access the Ethernet Disk RAID, the Console launches a Web browser, so the computer where you install the Console must have Microsoft Internet Explorer 6.0 or Firefox 1.06 or newer installed as well. In addition, one of those browsers must be your default browser. If you're not sure how to configure the default browser, refer to the documentation for your browser.

4.2. Starting the Console

Once you have installed the Console (as described in section 4.1. Installing the Console), use the following procedure to start it:

1. Click **Start** ➔ **Programs** ➔ **Storage System Console**.

   As soon as you start the Console, it automatically scans the network for storage devices. This might take a few minutes. As soon as the scan is complete, the left panel displays a tree view of all the storage devices it found.

   Each Ethernet Disk RAID has two ports for connecting to the network. If your Ethernet Disk RAID uses both ports, two items appear in the tree in the left pane, each using the same name. You can identify the IP address used by each port by clicking each item in the tree and observing the IP address area in the right pane.

2. In the left panel, select the name of the Ethernet Disk RAID that you want to access (for example, Storage), and then click **Log On Storage System Manager**. If your Ethernet Disk RAID uses both available ports to connect to the network, you can select either item.

   If your Ethernet Disk RAID has not yet been initialized, the **System Initialization** page appears. For more information, refer to section 3.2.3.

   If your Ethernet Disk RAID been initialized but not yet configured, the welcome page for the **System Set-up Wizard** appears. For more information, refer to section 4.4. Configuring with the First Use Wizard.

   If your Ethernet Disk RAID has been initialized and configured, the login page for the Manager appears. For more information, refer to section 5.2. Logging In to the Manager.

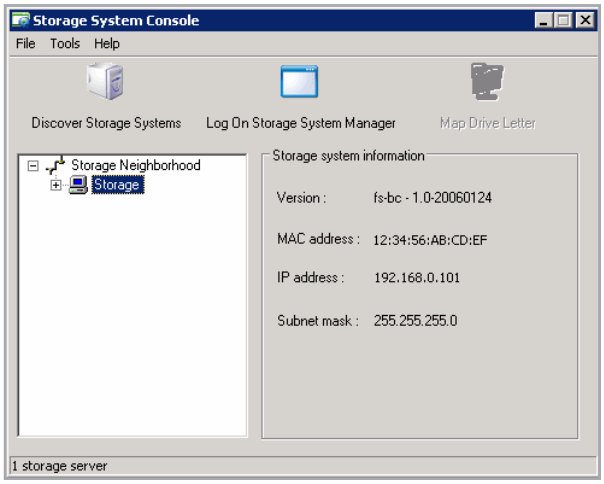


Fig. 4.2.

TECHNICAL NOTE: If you connect an Ethernet Disk RAID to the network after the Console has already scanned it, or if you subsequently change the IP address of the Ethernet Disk RAID, you must click **Discover Storage Systems** to scan the network again and update the tree in the left pane.

If no Ethernet Disk RAID appears in the left pane, your computer might not be in the same subnet as the Ethernet Disk RAID. Be sure to install the Console on a computer in the same subnet as the Ethernet Disk RAID and try again.

4.3. Initializing the Disks

Once you have installed the Console (as described in section 5.2. Logging In to the Manager), started it, and connected to the Ethernet Disk RAID (as described in section 4.2. Starting the Console), the System Initialization page appears (Fig. 4.3.).

If not all the hard disks have been detected, or if you want to add, remove, or re-order the disks at this time, insert or remove the disks one at a time and click Scan after each action.

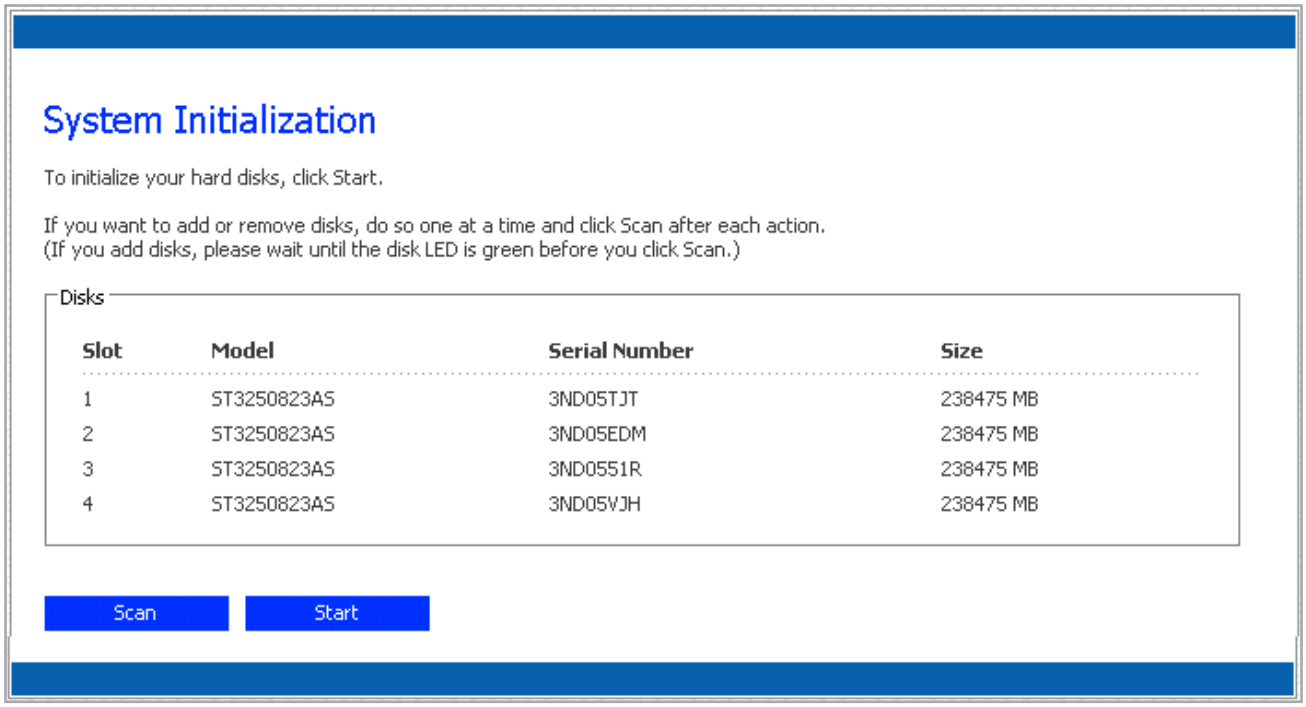

System Initialization
To initialize your hard disks, click Start.
If you want to add or remove disks, do so one at a time and click Scan after each action.
(If you add disks, please wait until the disk LED is green before you click Scan.)
Disks
Slot Model Serial Number Size
1 ST3250823AS 3ND05TJT 238475 MB
2 ST3250823AS 3ND05EDM 238475 MB
3 ST3250823AS 3ND0551R 238475 MB
4 ST3250823AS 3ND05VJH 238475 MB
Scan
Start

Fig. 4.3.

To initialize the hard disks:

1. Click Start. The firmware is uploaded to the hard disks. When this process is complete, the Ethernet Disk RAID will restart.
2. Close the browser window. After the system has restarted, you can perform initial configuration (as described in section 4.4. Configuring the Ethernet Disk RAID).

TECHNICAL NOTE: The operating system and Ethernet Disk RAID software are installed on each disk in your Ethernet Disk RAID to ensure that the failure or removal of any one disk will not cause the entire system to fail.

4.4. Configuring with the First Use Wizard

Once your Ethernet Disk RAID has been initialized (as described in section 4.3. Initializing the Ethernet Disk RAID), follow these steps to run the System Setup wizard and perform the necessary initial configuration:

1. If you have not already installed the Ethernet Disk RAID Console, install it (as described in section 4.1. Installing the Ethernet Disk RAID Console) and start it (as described in section 4.2. Starting the Console).

   In the left pane, click the name of the Ethernet Disk RAID. (If you're using both Ethernet ports, the name of the Ethernet Disk RAID appears twice in the left pane. You can click either one.) Then click **Log On Storage System Manager**.

   The welcome page appears (Fig. 3.3-A).

2. On the welcome page, click **Next**. The **End User Software License Agreement** page appears (Fig. 3.3-B).

3. If you agree to the terms, select the **I accept the license agreement** check box and then click **Next**. The **Host Name** page appears.

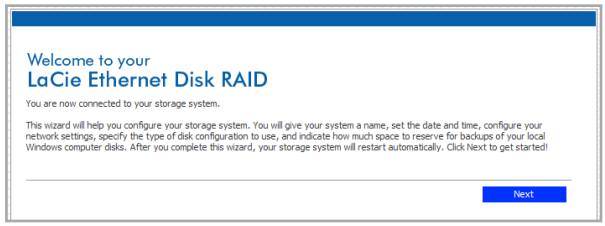

Welcome to your
LaCie Ethernet Disk RAID
You are now connected to your storage system.
This wizard will help you configure your storage system. You will give your system a name, set the date and time, configure your network settings, specify the type of disk configuration to use, and indicate how much space to reserve for backups of your local Windows computer disks. After you complete this wizard, your storage system will restart automatically. Click Next to get started!
Next

Fig. 4.4.A

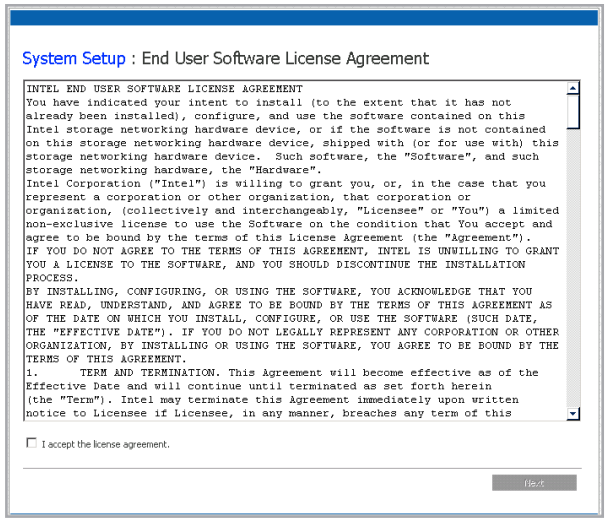

System Setup : End User Software License Agreement
INTEL END USER SOFTWARE LICENSE AGREEMENT
You have indicated your intent to install (to the extent that it has not already been installed), configure, and use the software contained on this Intel storage networking hardware device, or if the software is not contained on this storage networking hardware device, shipped with (or for use with) this storage networking hardware device. Such software, the "Software", and such storage networking hardware, the "Hardware".
Intel Corporation ("Intel") is willing to grant you, or, in the case that you represent a corporation or other organization, that corporation or organization, (collectively and interchangeably, "Licensee" or "You") a limited non-exclusive license to use the Software on the condition that You accept and agree to be bound by the terms of this License Agreement (the "Agreement").
IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, INTEL IS UNWILLING TO GRANT YOU A LICENSE TO THE SOFTWARE, AND YOU SHOULD DISCONTINUE THE INSTALLATION PROCESS.
BY INSTALLING, CONFIGURING, OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT AS OF THE DATE ON WHICH YOU INSTALL, CONFIGURE, OR USE THE SOFTWARE (SUCH DATE, THE "EFFECTIVE DATE"). IF YOU DO NOT LEGALLY REPRESENT ANY CORPORATION OR OTHER ORGANIZATION, BY INSTALLING OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT.
1. TERM AND TERMINATION. This Agreement will become effective as of the Effective Date and will continue until terminated as set forth herein (the "Term"). Intel may terminate this Agreement immediately upon written notice to Licensee if Licensee, in any manner, breaches any term of this
I accept the license agreement.
Next

Fig. 4.4.B

4. Click **Next** to accept the default name (Storage), or enter a name you prefer and then click **Next**. The name can be up to 15 characters long and can include letters, numbers, and hyphens. When you click **Next**, the **Date/Time** page appears (Fig. 4.4.C.).

5. Specify the current date, time, and time zone, and then click **Next**. The time should be expressed in 24-hour format. For example, 2:00 P.M. would be entered as 14:00:00. When you click **Next**, the **Network Settings** page appears (Fig. 4.4.D.).

6. By default, if your network has a DHCP server, the Ethernet Disk RAID obtains its IP address from that server.

   If your network does not have a DHCP server, the default IP address and subnet mask are used. (The default IP address is 192.168.0.101, and the default subnet mask is 255.255.255.0.).

   To accept the default settings, click **Next**. Otherwise, specify the desired settings and then click **Next**.

   When you click **Next**, the **Disk Configuration** page appears (see Fig. 4.4.E.). (The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.)

7. If you want to add or remove hard disks, do so one at a time and click **Scan** after each action.

   To accept the default disk configuration, RAID 5, click **Next**.

   RAID 5 provides the highest level of data protection, while RAID 5+ Spare provides the same protection and automatic data rebuilding in the event of a disk failure.

   If you want to change the disk configuration, select the desired RAID level and then click **Next**. (For detailed information about the different RAID levels, refer to section 10. RAID and Storage Policies.)

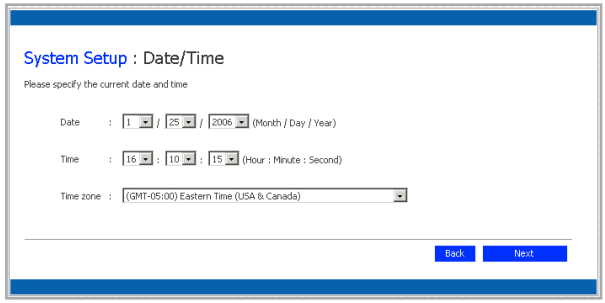

System Setup : Date/Time
Please specify the current date and time
Date : 1 / 25 / 2006 (Month / Day / Year)
Time : 16 : 10 : 15 (Hour : Minute : Second)
Time zone : (GMT-05:00) Eastern Time (USA & Canada)
Back
Next

Fig. 4.4.C.

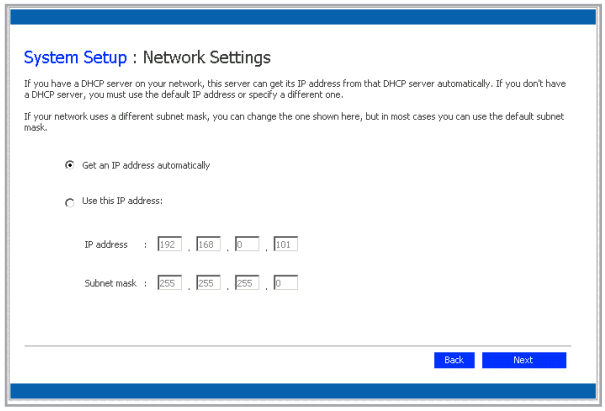

System Setup : Network Settings
If you have a DHCP server on your network, this server can get its IP address from that DHCP server automatically. If you don't have a DHCP server, you must use the default IP address or specify a different one.
If your network uses a different subnet mask, you can change the one shown here, but in most cases you can use the default subnet mask.
Get an IP address automatically
Use this IP address:
IP address : 192 . 168 . 0 . 101
Subnet mask : 255 . 255 . 255 . 0
Back
Next

Fig. 4.4.D.

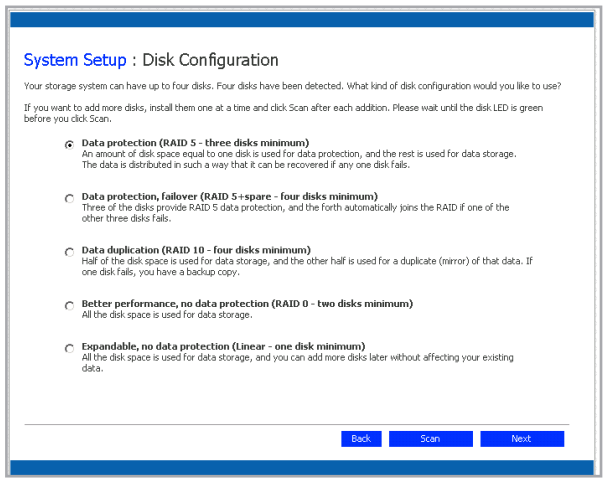

System Setup : Disk Configuration
Your storage system can have up to four disks. Four disks have been detected. What kind of disk configuration would you like to use?
If you want to add more disks, install them one at a time and click Scan after each addition. Please wait until the disk LED is green before you click Scan.
Data protection (RAID 5 - three disks minimum)
An amount of disk space equal to one disk is used for data protection, and the rest is used for data storage. The data is distributed in such a way that it can be recovered if any one disk fails.
Data protection, failover (RAID 5+spare - four disks minimum)
Three of the disks provide RAID 5 data protection, and the forth automatically joins the RAID if one of the other three disks fails.
Data duplication (RAID 10 - four disks minimum)
Half of the disk space is used for data storage, and the other half is used for a duplicate (mirror) of that data. If one disk fails, you have a backup copy.
Better performance, no data protection (RAID 0 - two disks minimum)
All the disk space is used for data storage.
Expandable, no data protection (Linear - one disk minimum)
All the disk space is used for data storage, and you can add more disks later without affecting your existing data.
Back
Scan
Next

Fig. 4.4.E.

CAUTION: RAID 0 and linear disk configurations do not offer any data protection. If you lose a hard disk, data loss will occur.

When you click **Next**, the **Disk Space Distribution** page appears (Fig. 4.4.F.).

8. To accept how the disk space will be proportioned for shared folders and backups (only 200 MB will be allocated for shared folders), click **Finish**.

   If you want to allocate more space for shared folders, select **Allocate more space for shared folders** and then specify how much space to allocate (either **All available disk space** or **Specified disk space**). If you select **Specified disk space**, enter the number of gigabytes to allocate for shared folders (the minimum is 1 GB). Then click **Finish**.

9. On the confirmation message, click **OK**. The **Configuration** page appears (see Fig. 4.4.G.) and the system is configured according to the settings you specified. Once the configuration is complete, the system restarts.

10. After the Ethernet Disk RAID restarts, you can access the Manager, add users, and create shared folders.

    For more information, refer to section 5.1. Accessing the Manager, section 5.2. Logging In to the Manager, section 5.4.1. Adding Users, and section 5.5.1. Creating Shared Folders.

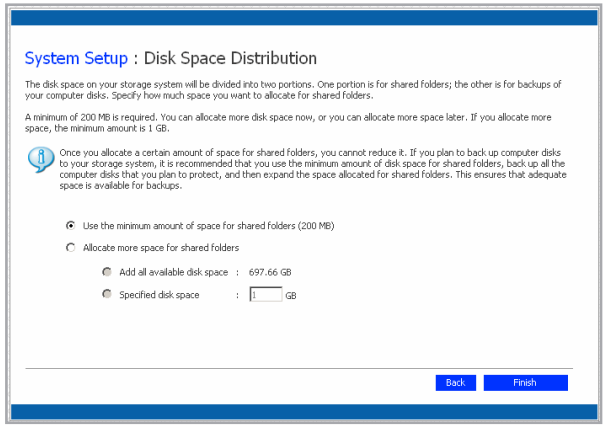

System Setup : Disk Space Distribution
The disk space on your storage system will be divided into two portions. One portion is for shared folders; the other is for backups of your computer disks. Specify how much space you want to allocate for shared folders.
A minimum of 200 MB is required. You can allocate more disk space now, or you can allocate more space later. If you allocate more space, the minimum amount is 1 GB.
Once you allocate a certain amount of space for shared folders, you cannot reduce it. If you plan to back up computer disks to your storage system, it is recommended that you use the minimum amount of disk space for shared folders, back up all the computer disks that you plan to protect, and then expand the space allocated for shared folders. This ensures that adequate space is available for backups.
Use the minimum amount of space for shared folders (200 MB)
Allocate more space for shared folders
Add all available disk space : 697.66 GB
Specified disk space : 1 GB
Back
Finish

Fig. 4.4.F.

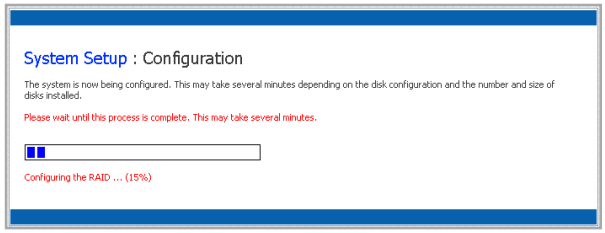

System Setup : Configuration
The system is now being configured. This may take several minutes depending on the disk configuration and the number and size of disks installed.
Please wait until this process is complete. This may take several minutes.
Configuring the RAID ... (15%)

Fig. 4.4.G.

IMPORTANT INFO: You can expand the amount of disk space allocated for shared folders later (as long as free disk space is available), but you cannot reduce it without re-configuring your disks and losing all your data. If you plan to back up computer disks to your Ethernet Disk RAID, it is recommended that you use the minimum amount of space for shared folders, back up all the computer disks that you plan to protect, and then expand the space allocated for shared folders. This ensures that adequate space is available for backups.

4.5. USB Devices

4.5.1. Attaching USB Devices

If you purchased optional USB external storage devices, you can attach them to the USB ports on the back of the unit (see (A) in Fig. 4.5.1.).

When you plug a USB device into the Ethernet Disk RAID, the device is automatically detected and is added to the USB page. (You might need to click **Scan** to update the display.)

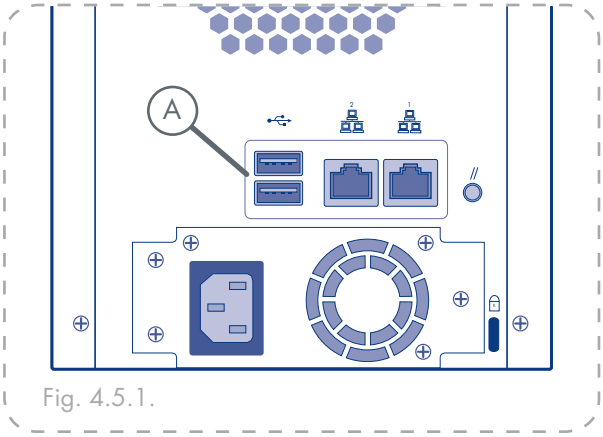


Fig. 4.5.1.

TECHNICAL NOTES:

- USB hubs are not supported.
- Any USB disk must be formatted before you use it with the Ethernet Disk RAID, and only the first partition of a FAT or FAT32 file system will be recognized.

4.5.2. Disconnecting USB Devices

The USB page displays a list of all USB devices that are currently attached to the Ethernet Disk RAID. USB disks are identified by the names usbdisk1 and usbdisk2. (These names cannot be changed.)

To unplug a USB device from the Ethernet Disk RAID, you must first use the Manager to disconnect it.

To disconnect a USB device:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **USB.**
3. In the list of USB devices, select the device(s) that you want to disconnect.
4. Click **Disconnect**.
5. When the confirmation message appears, click **OK**.

You can now unplug the USB device.

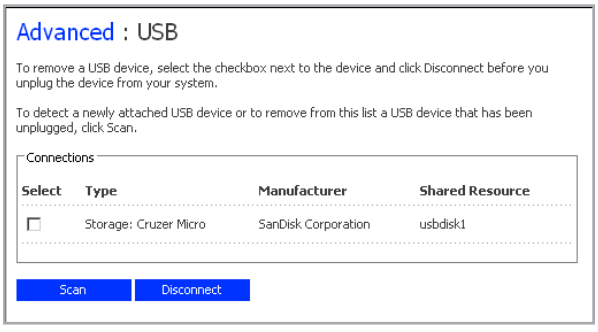

Advanced : USB
To remove a USB device, select the checkbox next to the device and click Disconnect before you unplug the device from your system.
To detect a newly attached USB device or to remove from this list a USB device that has been unplugged, click Scan.
Connections
Select
Type
Manufacturer
Shared Resource
Storage: Cruzer Micro
SanDisk Corporation
usbdisk1
Scan
Disconnect

Fig. 4.5.2.

TECHNICAL NOTE: If you inadvertently disconnect a USB device, unplug it from the Ethernet Disk RAID, plug it back in, and then click **Scan**. This reactivates the USB device. User assignments are always retained.

5. Managing Your LaCie Ethernet Disk RAID

The Web-based Manager enables you perform a number of tasks to help you get the most from your Ethernet Disk RAID:

- **Managing Users** – Add, modify, or remove users, or put users into groups.
- **Managing Shared Folders** – Create shared folders, rename existing shared folders, change which users can access existing shared folders or their access rights, and delete shared folders that you no longer want to keep.
- **Managing Backups** – View which computer disks are backed up, change the password for recovering a backup, specify which backup to remotely boot from, or delete a backup or backup client.
- **Setting Up e-mail Alerts** – Specify whether or not e-mail notifications should be sent when a problem occurs, and who should receive the notifications.
- **Upgrading the Firmware** – Upgrade your Ethernet Disk RAID firmware to the latest version.
- **Disconnecting USB Devices** – If you're using optional USB devices, you must disconnect them using the Manager before you physically unplug them.
- **Changing the System Settings** – Change the system name or time and date settings, as well as the user name or password for logging in to the Manager.
- **Changing the Network Settings** – Change the workgroup name, the Ethernet Disk RAID's IP address(es), or the gateway or DNS server settings, or enable the Ethernet Disk RAID to act as an FTP server.
- **Reconfiguring Your Disks** – Change the proportions of your Ethernet Disk RAID that are allocated to shared folders and backups, or change your disk configuration.
- **Viewing System Status Information** – See details about CPU and memory usage, how long the Ethernet Disk RAID has been running, disk temperatures, etc.
- **Logging Out of the Manager** – Log out of the Manager so that no one else can use your computer to make changes to the Ethernet Disk RAID.
- **Shutting Down the Ethernet Disk RAID** – Shut down using the Manager rather than pushing the power button manually.

5.1. Accessing the Manager

To access the Manager using the Console:

1. Start the Console and connect to the Ethernet Disk RAID (see section 4.2. Starting the Console).
2. Log in to the Manager (see section 5.2. Logging In to the Manager).

TECHNICAL NOTE: You can use the system name only if your computer is in the same subnet as the Ethernet Disk RAID, if you added the Ethernet Disk RAID's IP address and name to your local hosts file, or if you manually registered the name with a DNS server in your network.

To access the Manager using a Web browser:

1. From any computer in your network, run Microsoft Internet Explorer 6.0 or Firefox 1.06 or newer, enter the following in the address bar, and then press **Enter**:

   https://storage_system – where "storage_system" is the name or IP address of the Ethernet Disk RAID.

   When the login page appears, you can bookmark it so that you can quickly and easily access it the next time.

2. Log in to the Manager (see in section 5.2. Logging In to the Manager).

5.2. Logging In to the Manager

To ensure that your connection to the Ethernet Disk RAID is secure, the HTTPS protocol is used, and only individuals who know the administrator user name and password can view or change any of the Ethernet Disk RAID settings.

To log in to the Manager:

1. When the security alert appears, click **Yes**. The Login page appears.
2. Enter the administrator user name and password.
3. Click **Log In**.

The default administrator user name is **admin**, and the default password is **storage**. (These are case-sensitive.) However, you can change both the administrator user name and password at any time. For more information, refer to section 5.7.4. System.

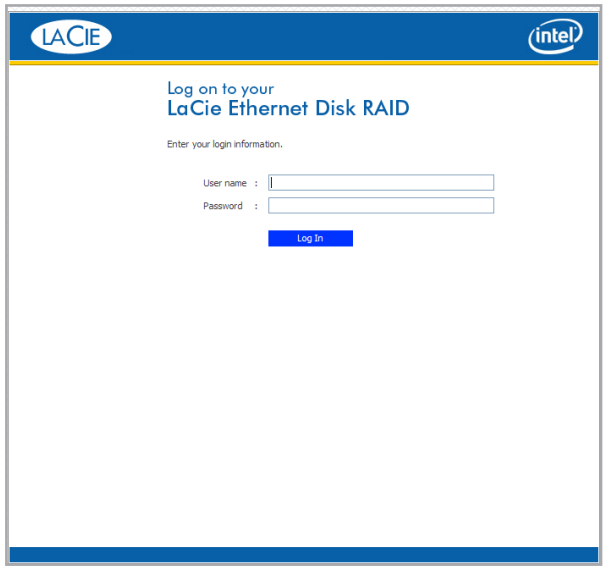


Fig. 5.2.

5.3. Navigating the Manager

Once you log in to the Manager, the **Home** page appears. The top of the **Home** page (and every page in the Manager) displays a navigation bar (Fig. 5.3.) that lets you access all the features of the Ethernet Disk RAID.

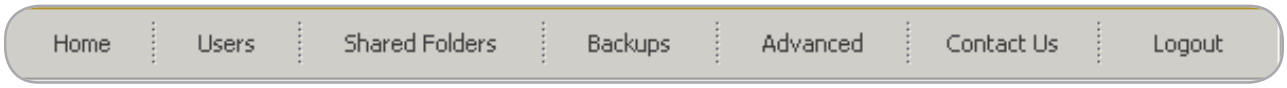


Fig. 5.3.

Menu Bar Access

Home

Displays information about your Ethernet Disk RAID, including how the storage space is being used and which users are connected. For more information, refer to section 5.3.1. Storage Status Tab and section 5.3.2. Connection Status Tab.

Users

Displays a list of all currently configured users and lets you add, modify, and remove users. For Windows and Mac OS X users, this area also lets you add, modify, and remove groups. For more information, refer to section 5.4.1. Adding Users and section 5.4. Managing Users.

Shared Folders

Displays a list of all currently configured shared folders and lets you add shared folders, change which users can access them, and remove them. For more information, refer to section 5.5.1. Creating Shared Folders and section 5.5. Managing Shared Folders.

Backups

Displays a list of all computer disk backups that currently exist and lets you change the recovery password, delete backups or a backup client, and change information related to booting remotely.
For more information, refer to section 5.6. Managing Backups and Section 7. Protecting Local Disks.

Advanced

Provides access to advanced Ethernet Disk RAID configuration options, such as setting up e-mail alerts; upgrading the firmware; removing USB devices; changing the system, network, or disk configuration settings; viewing information about system events; and shutting down the system remotely. For more information, refer to section 5.7. Advanced Management.

Contact Us

Provides a link to the LaCie technical support web site.

Log Out

Logs you out of the Manager.

5.3.1. Storage Status Tab

The Storage Status view displays information about the total storage capacity on the Ethernet Disk RAID, how much disk space is allocated for shared folders, how much is currently used by backups, and how much is available for either. (Initially, there is no used backup space. The information on this page changes as each computer backs up its hard disks to the Ethernet Disk RAID. You might have to refresh the browser window to reflect these changes.)

This page also indicates how much of the storage space allocated for shared folders is actually used, the total number of shared folders, and the number of networked computers (backup clients) that have backed up one or more disks on the Ethernet Disk RAID.

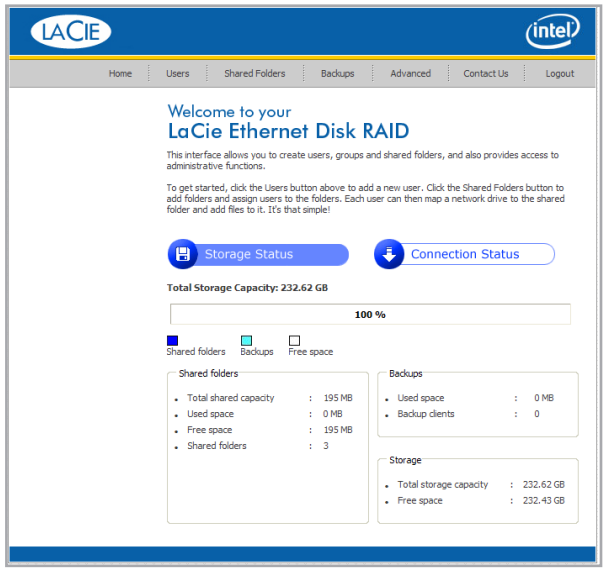

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
Welcome to your
LaCie Ethernet Disk RAID
This interface allows you to create users, groups and shared folders, and also provides access to administrative functions.
To get started, click the Users button above to add a new user. Click the Shared Folders button to add folders and assign users to the folders. Each user can then map a network drive to the shared folder and add files to it. It's that simple!
Storage Status
Connection Status
Total Storage Capacity: 232.62 GB
100 %
Shared folders
Backups
Free space
Shared folders
Total shared capacity : 195 MB
Used space : 0 MB
Free space : 195 MB
Shared folders : 3
Backups
Used space : 0 MB
Backup clients : 0
Storage
Total storage capacity : 232.62 GB
Free space : 232.43 GB

Fig. 5.3.1.

5.3.2. Connection Status Tab

The Connection Status Tab Displays a list of the Microsoft Windows and Mac OS X users who are currently connected to shared folders, including which shared folder they are accessing and when they logged on.

TECHNICAL NOTE: If anyone accessed a shared folder using the guest user name (which is described in more detail in section 5.4.1. Adding Users), guest appears in the Users column, followed in parentheses by the computer name.

Due to the nature of the NFS protocol, Linux and other Mac users are not listed on this page. Likewise, ongoing backup or recovery activities do not appear on this page.

This page indicates only that a connection with a shared folder has been established; this does not necessarily mean that the user has opened any files in the shared folder.

5.4. Managing Users

When you click **Users** in the navigation bar, the **Users & Computers** page appears. This page displays a list of all currently configured Windows and Mac OS X users, as well as all Linux and other Mac computers.

Only the individuals or computers that appear on this page can access the shared folders or back up their local hard disks on the Ethernet Disk RAID. You can add, modify, or remove users at any time.

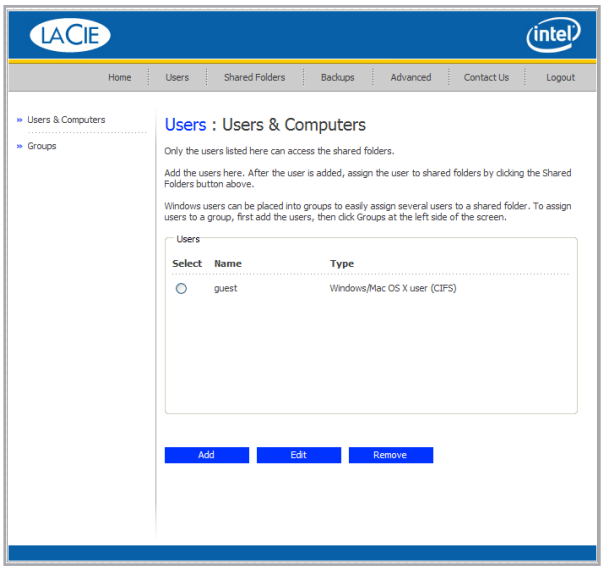

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
» Users & Computers
» Groups
Users : Users & Computers
Only the users listed here can access the shared folders.
Add the users here. After the user is added, assign the user to shared folders by clicking the Shared Folders button above.
Windows users can be placed into groups to easily assign several users to a shared folder. To assign users to a group, first add the users, then click Groups at the left side of the screen.
Users
Select
Name
Type
guest
Windows/Mac OS X user (CIFS)
Add
Edit
Remove

Fig. 5.4.

5.4.1. Adding Users

By default, the Ethernet Disk RAID includes a user named "guest" that has a password of "guest." Windows and Mac OS X users can access all shared folders that guest is authorized to access. However, you might want to add other users as well. For example, if you want to restrict access to a shared folder that contains confidential information, you would add at least one user and authorize that user to access that shared folder (and not authorize the guest user to access it). Adding a user for each individual or computer in your network provides flexibility and security, enabling you to control exactly who can access what information.

In addition, only Windows and Mac OS X users can use the guest user name. If there are Linux users or Mac users who aren't using OS X in your network, you must add users to allow those individuals to access any shared folders.

When you add a Windows or Mac OS X user, a folder with the same name as that person's user name is automatically created on the Ethernet Disk RAID. Only that person can access that folder and that person has full read/write access to it. (In the Console, this folder is identified as the home folder.)

You can add up to 64 Windows or Mac OS X users, and up to 64 Linux or other Mac users (for a total of up to 128 users).

See the next page for instructions on adding users.

TECHNICAL NOTE: Since each Linux/other Mac user can represent multiple users, the number of actual users can be higher.

To add a user:

1. In the navigation bar, click **Users**. The **Users & Computers** page appears (see Fig. 5.4.1.A.).
2. Click **Add**.
3. Select the type of user you want to add, and then click **Next**.

   The operating system used by the user determines which option you should choose – Windows/Mac OS X user (CIFS) or Linux/Other Mac user (NFS).

TECHNICAL NOTE: Linux users and Mac users who are not using OS X access shared folders using the Network File System (NFS). In this environment, access to shared folders is given to entire computers, not to individual users of those computers. However, in Windows and Mac OS X environments, each computer user can have individual access to a shared folder.

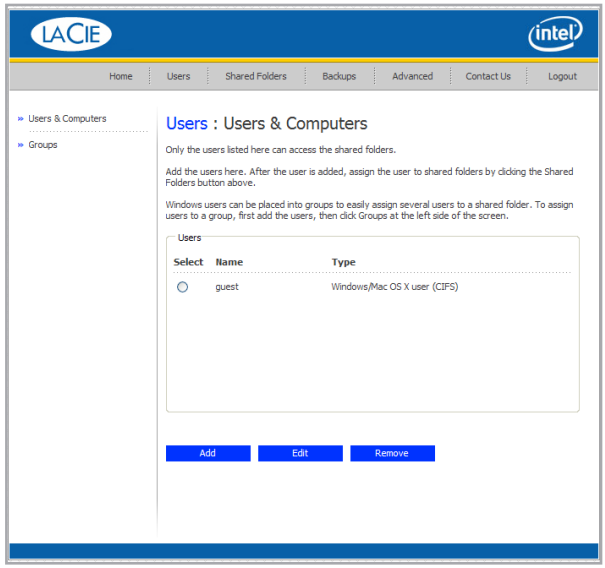

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
Users & Computers
Groups
Users : Users & Computers
Only the users listed here can access the shared folders.
Add the users here. After the user is added, assign the user to shared folders by clicking the Shared Folders button above.
Windows users can be placed into groups to easily assign several users to a shared folder. To assign users to a group, first add the users, then click Groups at the left side of the screen.
Users
Select
Name
Type
guest
Windows/Mac OS X user (CIFS)
Add
Edit
Remove

Fig. 5.4.1.A

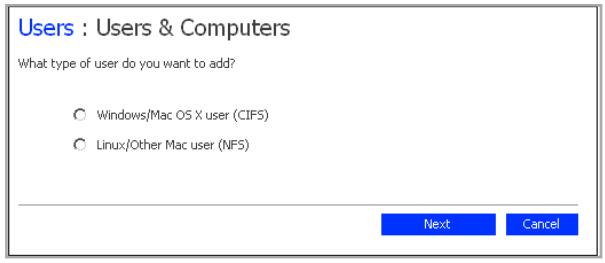
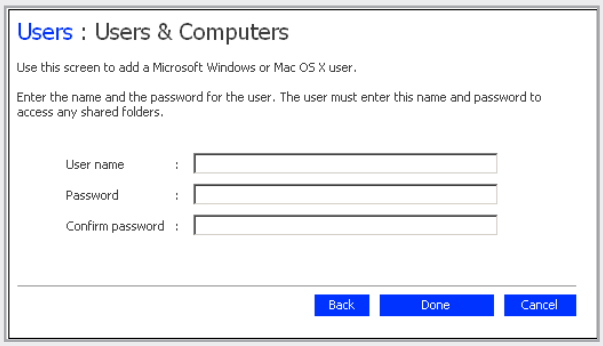


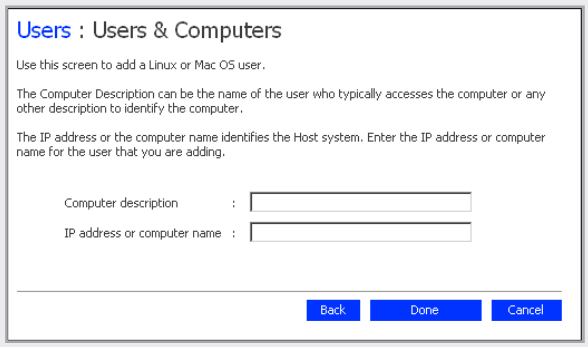
Fig. 5.4.1.B

The page that appears next varies, depending on the user type you selected:

■ Windows/Mac OS X User (CIFS)


Users : Users & Computers
Use this screen to add a Microsoft Windows or Mac OS X user.
Enter the name and the password for the user. The user must enter this name and password to access any shared folders.
User name :
Password :
Confirm password :
Back
Done
Cancel

■ Linux/Other Mac User (NFS)


Users : Users & Computers
Use this screen to add a Linux or Mac OS user.
The Computer Description can be the name of the user who typically accesses the computer or any other description to identify the computer.
The IP address or the computer name identifies the Host system. Enter the IP address or computer name for the user that you are adding.
Computer description :
IP address or computer name :
Back
Done
Cancel

4. Enter the requested user information and click **Done**.

Windows/Mac OS X Users (CIFS)

Enter the user name and password for accessing the shared folders. (You must enter the password a second time to confirm it.)

The user name can be up to 15 characters long and can include letters and numbers.

TECHNICAL NOTE: If the user name and password that you specify here are the same as the person's Windows user name and password, the person will not be prompted to provide a user name and password when accessing the shared folder.

Linux/Other Mac Users (NFS)

Enter a computer description and the IP address or computer name of the person's computer.

The Computer description can be the name of the person who typically uses the computer, or any other description that you want to provide to identify the computer in the Users list. This description can be up to 15 characters long. The IP address or computer name is the IP address or the actual computer name in the computer's system configuration.

TECHNICAL NOTE: You can create a single user that actually represents multiple users. In the IP address or computer name text box, you can use the wildcard characters * and ? to indicate a range of names. For example, client* or client? would include all computers in the subnet whose name begins with client. *.company.com would include all computers in the domain company.com. However, these wildcards cannot be used with IP addresses.

5. Repeat steps 2 through 4 until you have added all the users that you want to add at this time. (You can always add more users later.)

   If you'd like to put Windows and Mac OS X users into groups, refer to section 5.4.4. Working with Groups.

5.4.2. Modifying Users

For Windows and Mac OS X users, you can change the password used to access the shared folders, but not the user name. This change will not affect current connections, but will take effect the next time the person tries to connect to a shared folder.

For Linux and other Mac users, you can change the IP address or computer name, but not the computer description. Changing this information immediately disconnects that computer from the shared folders.

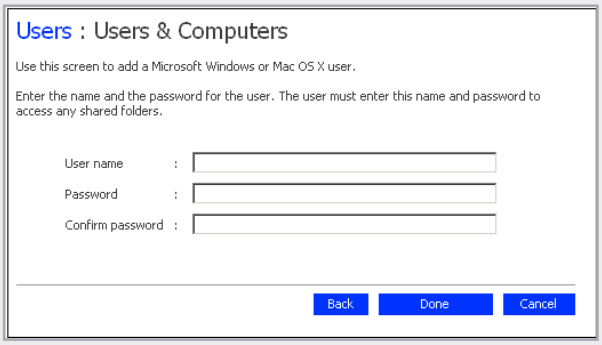
TECHNICAL NOTE: To change the user name or computer description, you must remove the existing user as described in section 5.4.3. Removing Users, and then add a new user with the desired name or description as described in section 5.4.1. Adding Users.

To modify a user:

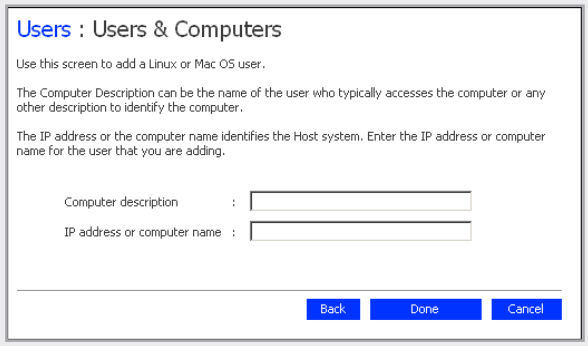
1. In the navigation bar, click **Users**.
2. Select the radio button next to the user that you want to modify.
3. Click **Edit**.

The page that appears next varies, depending on the type of user you selected.

Windows/Mac OS X User (CIFS)


Users : Users & Computers
Use this screen to add a Microsoft Windows or Mac OS X user.
Enter the name and the password for the user. The user must enter this name and password to access any shared folders.
User name :
Password :
Confirm password :
Back
Done
Cancel

Linux/Other Mac User (NFS)


Users : Users & Computers
Use this screen to add a Linux or Mac OS user.
The Computer Description can be the name of the user who typically accesses the computer or any other description to identify the computer.
The IP address or the computer name identifies the Host system. Enter the IP address or computer name for the user that you are adding.
Computer description :
IP address or computer name :
Back
Done
Cancel

4. Make the desired change and click **OK**.

Windows/Mac OS X Users (CIFS)

Enter the password for accessing the shared folders. (You must enter the password a second time to confirm it.)

TECHNICAL NOTE: If the user name and password specified here are the same as the person's Windows user name and password, the person will not be prompted to provide a user name and password when accessing the shared folders.

Linux/Other Mac Users (NFS)

Enter the computer's IP address or the actual computer name in the computer's system configuration.

A single user can actually represent multiple computers. In the IP address or computer name text box, you can use the wildcard characters * and ? to indicate a range of names. For example, client* or client? would include all computers in the subnet whose name begins with client. *.company.com would include all computers in the domain company.com. However, these wildcards cannot be used with IP addresses.

TECHNICAL NOTE: If the user is currently connected to a shared folder, changing this information will disconnect the user.

5.4.3. Removing Users

You can remove any user except the "guest" user.

If you remove a user who is currently connected to the Ethernet Disk RAID, that user remains connected until the user disconnects from the shared folder or shuts down the computer.

To remove a user:

1. In the navigation bar, click **Users**.
2. Select the radio button next to the user that you want to remove.
3. Click **Remove**.
4. When prompted to confirm the removal, click **OK**.

The user no longer appears in the list on the **Users** page.

CAUTION: When you remove a Windows/Mac OS X user, that user's personal (home) folder is automatically deleted. If you're removing the user simply to change the person's user name, you might want to have the user copy any data from this folder to another location to ensure that it is not lost.

5.4.4. Working with Groups

Windows and Mac OS X users can be put into groups, which makes it easier to give several users access to the same shared folder at once.

When you click **Users** in the navigation bar and click **Groups** in the left pane, the page displays a list of all currently configured groups. When you select a group in the **Groups** list, the members of that group appear in the adjacent **Members** list.

You can add a group, modify the group membership, or remove groups at any time.

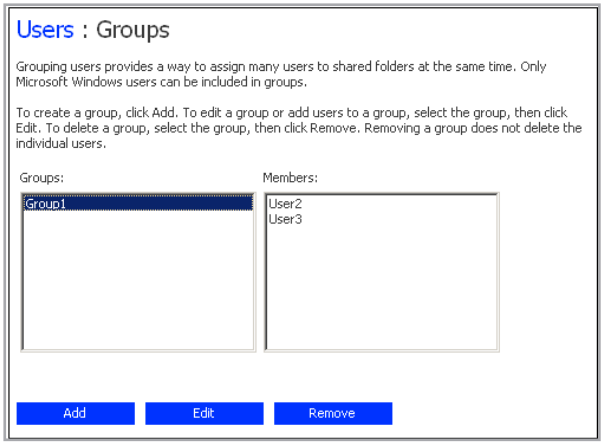

Users : Groups
Grouping users provides a way to assign many users to shared folders at the same time. Only Microsoft Windows users can be included in groups.
To create a group, click Add. To edit a group or add users to a group, select the group, then click Edit. To delete a group, select the group, then click Remove. Removing a group does not delete the individual users.
Groups:
Members:
Group1
User2
User3
Add
Edit
Remove

Fig. 5.4.4.

5.4.4.1. Adding a Group

Windows and Mac OS X users can also be put into groups. Putting users into groups makes it easier to give several users access to the same shared folder at once. Each user can be a member of multiple groups.

When you create a group, you typically specify which users should be members of that group, although you can create an empty group and add users later. (You must add users as described in section 5.4.1. Adding Users before you can add those users to a group.)

Each user can be a member of multiple groups. For example, the user Alice might be a member of both the Marketing and Executives groups.

You can create up to 16 groups.

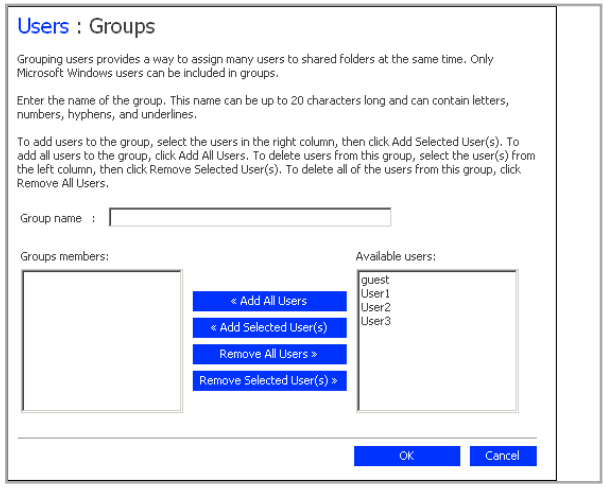

Users : Groups
Grouping users provides a way to assign many users to shared folders at the same time. Only Microsoft Windows users can be included in groups.
Enter the name of the group. This name can be up to 20 characters long and can contain letters, numbers, hyphens, and underlines.
To add users to the group, select the users in the right column, then click Add Selected User(s). To add all users to the group, click Add All Users. To delete users from this group, select the user(s) from the left column, then click Remove Selected User(s). To delete all of the users from this group, click Remove All Users.
Group name :
Groups members:
Available users:
guest
User1
User2
User3
« Add All Users
« Add Selected User(s)
Remove All Users »
Remove Selected User(s) »
OK
Cancel

Fig. 5.4.4.1.

To add a group:

1. In the navigation bar, click **Users**.
2. In the left pane, click **Groups**.
3. Click **Add**.
4. In the **Group name** text box, enter a unique name for the group.

   This name can be up to 15 characters long and can include letters, numbers, hyphens, and underlines.

5. Specify which users should belong to this group, and then click **OK**. See the table, below.

TECHNICAL NOTE: To select multiple, contiguous users, hold down the **Shift** key and select the first user, then select the last user. All users between the first and last selected user are selected. To select multiple, non-contiguous users, hold down the **Ctrl** key as you select each user.

To accomplish this	Do this
Add all users to the group	Click **Add All Users**. All users move from the Available users list to the Group members list.
Add selected users to the group	In the Available users list, select the user(s) that you want to add and then click **Add Selected User(s)**.
Remove all users from the group	Click **Remove All Users**. All users move from the Group members list to the Available users list.
Remove selected users from the group	In the Group members list, select the user(s) that you want to remove from the group and then click **Remove Selected User(s)**.

5.4.4.2. Changing the Group Membership

You can change which users are members of each group at any time. When you add a user to a group, that user immediately has access to all the shared folders that the group is authorized to access. However, if you remove a user from a group, the change does not take effect until that user disconnects from the shared folder or shuts down the computer.

To change the group membership:

1. In the navigation bar, click **Users**.
2. In the left pane, click **Groups**.
3. In the **Groups** list, select the group whose membership you want to change.
4. Click **Edit**.
5. Specify which users should belong to this group, and then click **OK**. See the table, below.

   The selected users move from one list to the other.

   On the Groups page, when you select this group in the Groups list, the adjacent Members list immediately reflects the changes you just made.

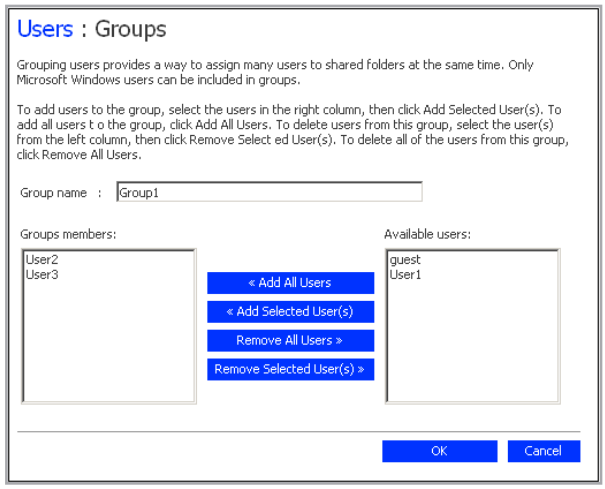

Users : Groups
Grouping users provides a way to assign many users to shared folders at the same time. Only Microsoft Windows users can be included in groups.
To add users to the group, select the users in the right column, then click Add Selected User(s). To add all users t o the group, click Add All Users. To delete users from this group, select the user(s) from the left column, then click Remove Select ed User(s). To delete all of the users from this group, click Remove All Users.
Group name :
Group1
Groups members:
User2
User3
« Add All Users
« Add Selected User(s)
Remove All Users »
Remove Selected User(s) »
Available users:
guest
User1
OK
Cancel

Fig. 5.4.4.2.

TECHNICAL NOTE: To select multiple, contiguous users, hold down the **Shift** key and select the first user, then select the last user. All users between the first and last selected user are selected. To select multiple, non-contiguous users, hold down the **Ctrl** key as you select each user.

■ Group Options	
To accomplish this	**Do this**
Add all users to the group	Click **Add All Users**. All users move from the **Available users** list to the **Group members** list.
Add selected users to the group	In the **Available users** list, select the user(s) that you want to add and then click **Add Selected User(s)**.
Remove all users from the group	Click **Remove All Users**.
Remove selected users from the group	In the **Group members** list, select the user(s) that you want to remove from the group and then click **Remove Selected User(s)**.

5.4.4.3. Removing a Group

1. In the navigation bar, click **Users**.
2. In the left pane, click **Groups**.
3. In the **Groups** list, select the group that you want to remove.
4. Click **Remove**.
5. When prompted to confirm the removal, click **OK**.

   The group no longer appears in the **Groups** list.

TECHNICAL NOTE: Removing a group does not remove the users that are members of that group; it simply means that the group will no longer appear in the Groups list on the Groups page. The users remain listed on the Users & Computers page.

However, removing a group can affect access to shared folders. When you remove a group, the members of that group will no longer have access to any shared folders that the group was authorized to access unless they were granted individual access as well.

5.5. Managing Shared Folders

When you click Shared Folders in the navigation bar, the page displays a list of all shared resources, including both shared folders and USB devices. When you select an item in the

Shared folders list, the users and groups that can access that item appear in the Users with access list. (For groups, the group name is preceded by an @ symbol.)

By default, the Ethernet Disk RAID includes a shared folder named public, and all Windows and Mac OS X users can access it and create, modify, or delete files there (unless you change the list of authorized users or their access rights as described in section 5.5.2. Changing User Access to Shared Folders).

In addition, when you add a Windows/Mac OS X user (as described in section 5.4.1. Adding Users), the Ethernet Disk RAID automatically creates a shared folder with the same name as the person's user name. However, these shared folders do not appear in the Shared folders list.

You can create additional shared folders and delete them at any time. For both shared folders and USB disks, you can change which users can access them and what they can do with the subfolders and files there.

5.5.1. Creating Shared Folders

By default, the LaCie Ehternet Disk RAID includes a shared folder named public, which all Windows and Mac OS X users can access (unless you change the list of authorized users or their access rights as described in section 5.5.2. Changing User Access to Shared Folders).

In addition, when you add a Windows or Mac OS X user (as described in section 5.4.1. Adding Users), the Ethernet Disk RAID automatically creates a shared folder with the same name as the person's user name. Only that user can access that shared folder (as described in section 6.1. Accessing Shared Folders).

You can create up to 32 shared folders. Users who can access and write to these shared folders can create additional sub-folders for organizing the files they store there.

To create a shared folder:

1. In the navigation bar, click **Shared Folders**. The **Shared Folders** page appears (see Fig. 5.5.1.A).
2. Click **Add**.

TECHNICAL NOTE: The Shared folders list includes usbdisk1 and usbdisk2 whether or not any USB disks have been connected to the Ethernet Disk RAID. Shared folders created as a result of adding Windows/Mac OS X users do not appear in the Shared folders list.

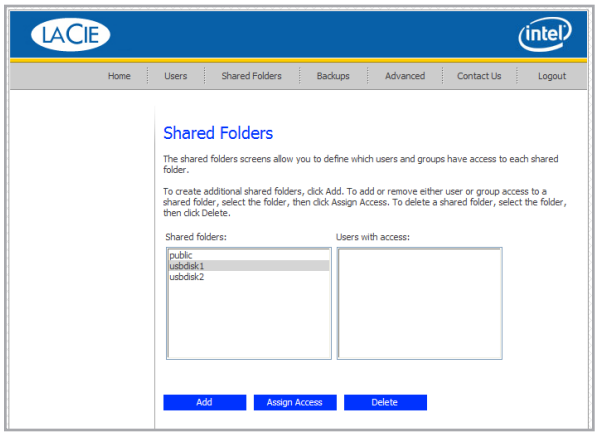

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
Shared Folders
The shared folders screens allow you to define which users and groups have access to each shared folder.
To create additional shared folders, click Add. To add or remove either user or group access to a shared folder, select the folder, then click Assign Access. To delete a shared folder, select the folder, then click Delete.
Shared folders:
Users with access:
public
usbdisk1
usbdisk2
Add
Assign Access
Delete

Fig. 5.5.1.A.

3. Specify which type of user will be accessing this shared folder, and then click **Next**.

4. In the **Shared folder name** text box (Fig. 5.5.1.C), enter a unique name for the shared folder, and then click **Next**.

   This name can be up to 64 characters long and can contain letters, numbers, hyphens, underlines and spaces.

TECHNICAL NOTE: Each shared folder name must be unique. For example, if you create a shared folder named Photos for Windows/Mac OS X users, you cannot subsequently create a shared folder named Photos for Linux/other Mac users. In addition, the shared folder name cannot be the same as any Windows/Mac OS X user name.

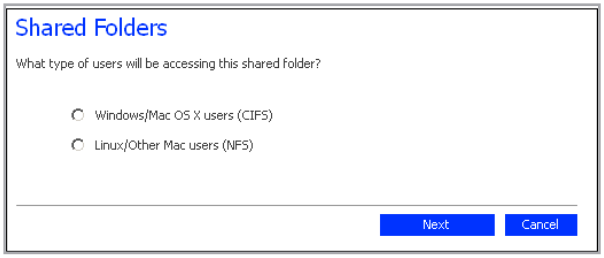


Fig. 5.5.1.B

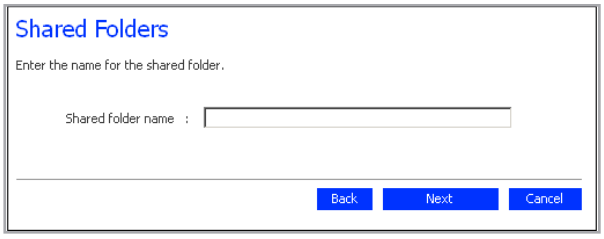
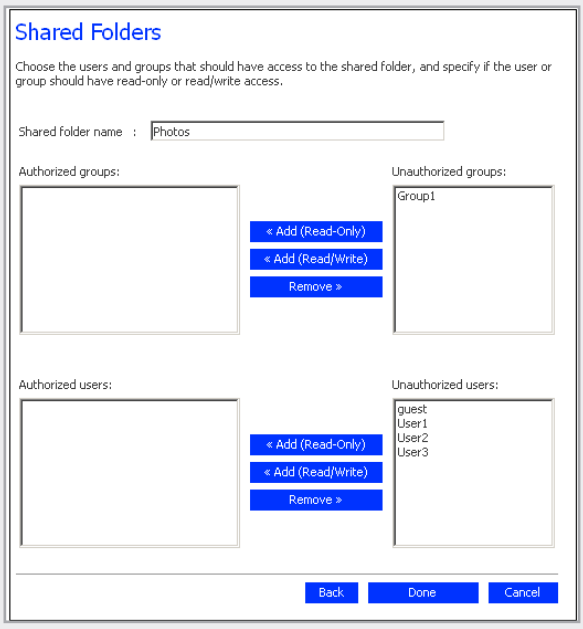


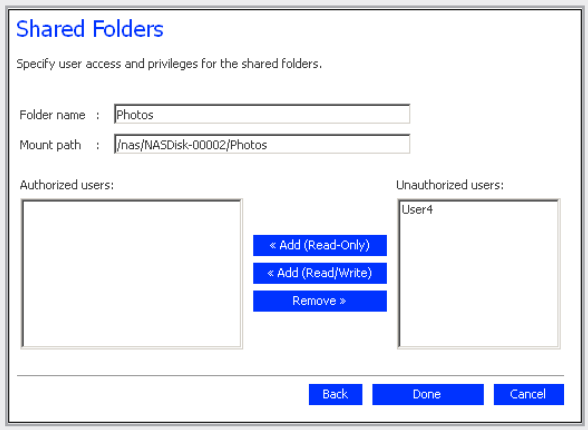
Fig. 5.5.2.C

The page that appears next varies, depending on the user type you selected.

■ Windows/Mac OS X User (CIFS)



■ Linux/Other Mac User (NFS)



5. In the **Unauthorized users** list, select the name of the user who should be able to access this shared folder
6. Then specify what access rights the selected user(s) should have: read-only or write-only.

   The selected user(s) move from the **Unauthorized users** list to the **Authorized users** list.

   If you accidentally add a user that you didn't mean to add, select the user in the **Authorized users** list and click **Remove**. The user returns to the Unauthorized users list.
7. Repeat step 5 until you have defined access rights for all the desired users and groups, and then click **Done**.
8. Repeat steps 2 through 6 until you have created all the shared folders that you want to create at this time. (You can always create more shared folders later.)

When you have finished, you can log out (as described in section 5.8. Logging Out of the Manager), or you can explore more of the features that the Ethernet Disk RAID has to offer. (For more information, refer to Section 5.7. Advanced Management.)

TECHNICAL NOTE: If you created groups (as described in section 5.4.4.1. Adding a Group), you can perform this step with the **Unauthorized groups** list.

This page shows all groups and all users. For example, if you created a group named Group1, and added User2 and User3 to that group, the Unauthorized groups list includes Group1, and the Unauthorized users list includes User2 and User3. If you select Group1 and click Add (Read-Only), Group1 moves to the Authorized groups list, but User2 and User3 do not move to the Authorized users list. This allows you to specify unique access rights for those users. For example, you could select User3 and click Add (Read/Write). This would mean that everyone in Group1 would have read-only access to the shared folder except User3, who would have read/write access to it.

On the Shared Folders page, the group name in the Users with access column is preceded by an @ symbol.

5.5.2. Changing User Access to Shared Folders

You can change which users can access any folder or USB disk and what level of access they have. (Shared folders that are created as a result of creating Windows/Mac OS X users do not appear in the Shared folders list and cannot be modified. These folders automatically provide only the associated user with read/write access to that folder.)

When you add a user to the list of authorized users for a shared folder or USB disk, that change takes effect immediately. However, if you remove a user from the list of authorized users, or if you change the user's access rights, the change does not take effect until that user disconnects from the shared folder or USB disk, or shuts down the computer.

To change user access to shared folders and USB disks:

1. In the navigation bar, click **Shared Folders**.
2. In the **Shared folders** list, select the shared folder or USB disk whose user access you want to change.
3. Click **Assign Access**.
4. If you selected a shared folder or a USB disk to which you previously assigned users, go to step 5.

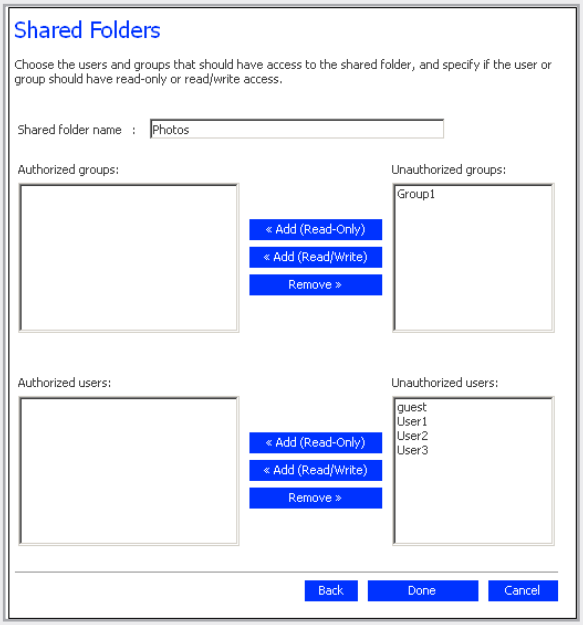
   If you selected a USB disk to which you did not previously assign users, select the type of user that you want to assign to this USB disk, and then click **Next**.

TECHNICAL NOTE: By default, all users have read/write access to the public folder. You can change the user assignments or access rights for the public folder.

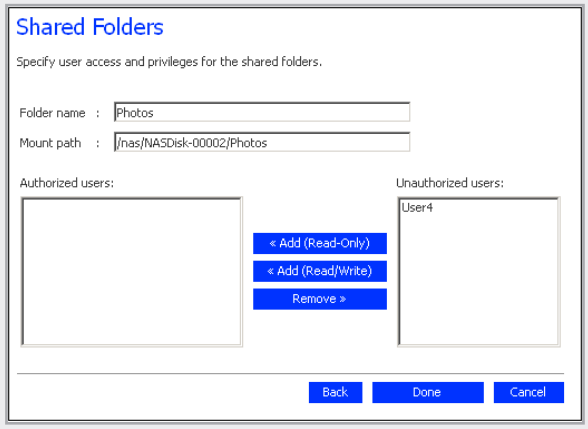
TECHNICAL NOTE: Linux user and Mac users who are not using OS X access shared folders using NFS. In this environment, access to shared folders is given to entire computers, not to individual users of those computers. However, in Windows and Mac OS X environments, each computer user can have individual access to a shared folder.

The page that appears next varies, depending on what type of users can access the shared folder you selected.

Windows/Mac OS X User (CIFS)



Linux/Other Mac User (NFS)



5. Specify which users should be able to access this shared folder or USB disk, and then click **OK**. See the table, below.

   The selected users move from one list to the other.

Shared Folder Access Options

To accomplish this	Do this
Allow selected users access to the shared folder or USB disk	In the **Unauthorized users** list, select the user(s) who should be able to access the shared resource and then click **Add (Read-Only)** or **Add (Read/Write)**. Users with read-only access can only view the files in the shared resource; users with read/write access can view, add, modify, and delete folders and files in the shared resource.
Prevent selected users from accessing the shared folder or USB disk	In the **Authorized users** list, select the user(s) who should not be able to access the shared resource and then click **Remove**.

TECHNICAL NOTE:

- If you created groups (as described in section 5.4.4.1. Adding a Group), you can perform this step with groups as well.

  This page shows all groups and all users. For example, if you created a group named Group1, and added User2 and User3 to that group, the **Unauthorized groups** list includes Group1, and the **Unauthorized users** list includes User2 and User3. If you select Group1 and click **Add (Read-Only)**, Group1 moves to the **Authorized groups** list, but User2 and User3 do not move to the **Authorized users** list. This allows you to specify unique access rights for those users. For example, you could select User3 and click **Add (Read/Write)**. This would mean that everyone in Group1 would have read-only access to the shared folder except User3, who would have read/write access to it.

5.5.3. Deleting a Shared Folder

Once you have created a shared folder, you can delete it at any time. When you delete a shared folder, any users who are currently accessing it are immediately disconnected from it.

To delete a shared folder:

1. In the navigation bar, click **Shared Folders**.
2. In the **Shared folders** list, select the shared folder that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the deletion, click **OK**.

   The shared folder no longer appears in the **Shared Folders** list, and all associated subfolders and files are deleted.

CAUTION: Deleting a shared folder deletes all the subfolders and files in that shared folder. If you want to delete only selected subfolders or files, access the shared folder (as described in section 6.1. Accessing Shared Folders) and delete the desired items.

TECHNICAL NOTES:

- You cannot delete the public folder or any folders created automatically as a result of adding Windows/Mac OS X users (which do not appear on the Shared Folders page).
- You cannot delete the contents of a USB disk using the Shared Folders page. To delete its contents, you must give yourself read/write access to that disk (as described in section 5.5.2. Changing User Access to Shared Folders), access the disk (as described in section 6.1. Accessing Shared Folders), and then delete the desired folders and files.

  To remove the USB disk from the Ethernet Disk RAID, use the Manager to disconnect it (as described in section 4.5.2. Disconnecting USB Devices). Then physically unplug the USB disk from the Ethernet Disk RAID. Even after you physically unplug the USB disk, it remains in the Shared folders list.

5.6. Managing Backups

Once the users have used Windows Backup Software to back up their computer hard disks to the Ethernet Disk RAID (as described in section 7. Protecting Local Disks), the Backups page displays a list of each computer that has done this, the size of each protected disk, the date and time of all available backups, and the backup disk ID (the number used to identify the backup on both the storage server and on the Status page in the Windows Backup Software software).

If a user ever has to recover a disk using the recovery CD or remotely boot from a backup on the Ethernet Disk RAID, the user will be prompted for a password to do so. The user had to provide this password when protecting the disk. However, if the user forgets it, you can reset the password using the Manager. (For information about recovering a disk using the recovery CD, refer to section 7.9.3. Recovering a System Disk Using the Recovery CD. For information about booting remotely, refer to section 7.9.4. Recovering a System Disk While Booting Remotely.)

For booting remotely, you can also specify the MAC address to use (if you want to remotely boot a computer using a different computer's backup) and the backup to boot from.

In addition, when a user removes protection for a disk, the existing backups are not deleted. The user can re-use the allocated space for new backups, or you can delete those backups manually using the Manager.

5.6.1. Changing the Recovery Password

1. In the navigation bar, click **Backups**.
2. In the **Computer name** list in the **Recovery passwords** group box, select the name of the computer whose recovery password you want to change.
3. In the **Recovery password** text box, type the password to use. This password must be 12-16 characters long.
4. Click **Change Password**.
5. When the confirmation message appears, click **OK**.

The user must provide this password when recovering a disk from this Ethernet Disk RAID using the Recovery CD or when remotely booting from a backup on the Ethernet Disk RAID.

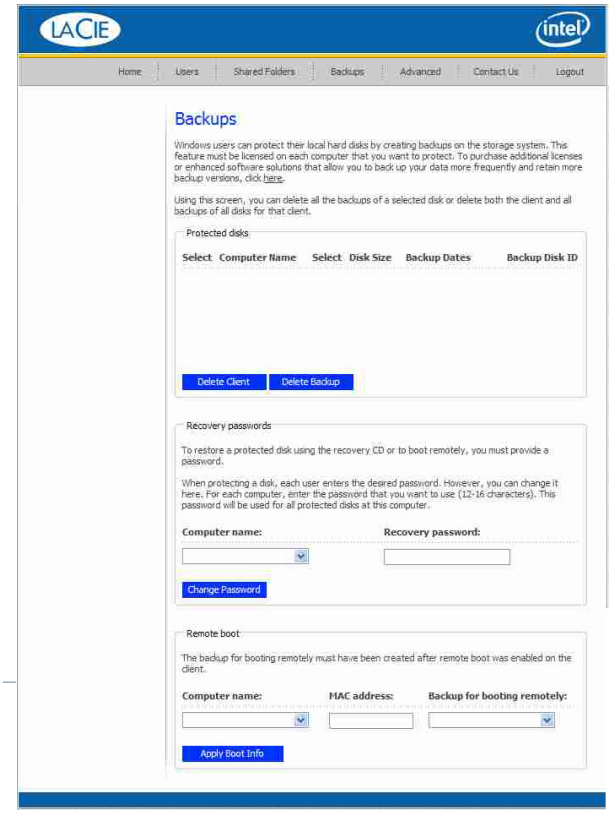

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
Backups
Windows users can protect their local hard disks by creating backups on the storage system. This feature must be licensed on each computer that you want to protect. To purchase additional licenses or enhanced software solutions that allow you to back up your data more frequently and retain more backup versions, click here.
Using this screen, you can delete all the backups of a selected disk or delete both the client and all backups of all disks for that client.
Protected disks
Select
Computer Name
Select
Disk Size
Backup Dates
Backup Disk ID
Delete Client
Delete Backup
Recovery passwords
To restore a protected disk using the recovery CD or to boot remotely, you must provide a password.
When protecting a disk, each user enters the desired password. However, you can change it here. For each computer, enter the password that you want to use (12-16 characters). This password will be used for all protected disks at this computer.
Computer name:
Recovery password:
Change Password
Remote boot
The backup for booting remotely must have been created after remote boot was enabled on the client.
Computer name:
MAC address:
Backup for booting remotely:
Apply Boot Info

Fig. 5.6.1.

5.6.2. Configuring Remote Boot

Normally, when you enable remote boot for a client computer (as described in section 7.8.1. Enabling Remote Boot), no additional action is necessary on the Ethernet Disk RAID.

However, if you want to remotely boot one computer from another computer's backup, you must change the MAC address. For example, if Computer1 has been infected by a virus, and all of its backups are also infected, you might want to boot Computer1 from one of Computer2's backups and recover that disk to Computer1. To do this, you must change the MAC address associated with Computer2.

You can also specify which backup to remotely boot from. By default, you always boot from the latest backup. (You can boot from an earlier backup, but no matter which backup you boot from, you can recover only the latest backup.)

To configure remote boot:

1. In the navigation bar, click **Backups**.
2. In the **Computer name** list in the **Remote boot group** box, select the name of the computer whose backup you want to remotely boot from.
3. If you're remotely booting the computer from its own backup, do not change the MAC address. However, if you're booting a different computer from the selected computer's backup, enter the MAC address of the NIC of the computer that you want to remotely boot in the **MAC address** text box.

   Remote boot must have been previously enabled on that computer.
4. From the **Backup for booting remotely** list, select the time and date of the backup that you want to remotely boot from. To always boot from the most recent backup, select **Latest backup**. An asterisk (*) identifies the backup that will be used for booting remotely.
5. Click **Apply Boot Info**.
6. When the confirmation message appears, click **OK**.

   If you changed the backup for booting remotely, an asterisk now appears next to the selected backup.

IMPORTANT INFO: If you try to recover one computer from another computer's backup, both computers must have identical hardware. Otherwise, the recovered files will not operate properly.

TECHNICAL NOTES:

- You can remotely boot only from backups that were created after remote boot was enabled on the client computer.
- If the selected backup is deleted to make room for newer backups, the most recent backup will be used for booting remotely.

5.6.3. Deleting a Backup

You can delete all backups of a given disk, but you cannot delete just an individual backup from a specific date and time.

To delete all backups of a disk:

1. In the navigation bar, click **Backups**.
2. Select the radio button adjacent to the disk whose backups you want to delete (in the second **Select** column).
3. Click **Delete Backup**.
4. When prompted to confirm the deletion, click **OK**.

   The disk no longer appears on the **Backups** page, and all backup versions are deleted.

   If only one disk was protected, the computer name disappears from the page as well.

IMPORTANT INFO: If you delete all backups of all disks for a particular computer, that computer no longer appears on the Backups page. However, that computer name remains in the Ethernet Disk RAID and counts toward the total number of computers that are allowed to back up to the Ethernet Disk RAID. If you want to delete all backups of all disks and the computer name, refer to section 5.6.4. Deleting a Client.

TECHNICAL NOTE: If you delete a backup and the user did not previously remove protection for that disk, when the user subsequently accesses Client Backup and Recovery, the Status page will indicate that the backup of the protected disk is offline. To back up the disk once again, the user must remove protection and then protect the disk again. For more information, refer to section 7.9.5. Removing Protection and section 7.2. Protecting Your Disks.

5.6.4. Deleting a Client

If you remove the Windows Backup Software software from a particular computer, or if you change the computer name, the original computer name remains on the Ethernet Disk RAID and counts toward the total number of computers that are allowed to back up to the Ethernet Disk RAID. To both delete all backups of all disks for a particular computer and the computer name, you must delete the client.

To delete a client:

1. In the navigation bar, click **Backups**.
2. Select the radio button to the left of the computer whose backups and computer name you want to delete from the Ethernet Disk RAID (in the first Select column).
3. Click **Delete Client**.
4. When prompted to confirm the deletion, click **OK**.

All backups of all disks associated with this computer are deleted, and the computer name is also deleted from the Ethernet Disk RAID.

TECHNICAL NOTE: If you delete a client and the user did not previously remove protection for that disk, when the user subsequently accesses the Windows Backup Software software, the Status page will indicate that the backup of the protected disk is offline. To back up the disk once again, the user must remove protection and then protect the disk again. For more information, refer to section 7.9.5. Removing Protection and section 7.2. Protecting Your Disks.

5.7. Advanced Management

5.7.1. Alerts

The **Alerts** page allows you to set up the Ethernet Disk RAID to notify up to three people via email if a problem occurs—for example, if one of the disks fails, or if insufficient space is available for creating new files or performing a backup.

To take advantage of this feature, you must have access to an SMTP e-mail server either within your own network or through an Internet service provider.

To set up e-mail alerts:

1. In the navigation bar, click **Advanced**.
2. On the Advanced page, click **Alerts**.
3. Specify whether or not the Ethernet Disk RAID should send e-mail notifications when a problem occurs by selecting or clearing the **Send e-mail notifications** check box.

   If you select this option, you must provide the fully qualified domain name or IP address of your e-mail server and at least one e-mail address.

   If you clear this option, e-mail notifications will not be sent, and all the related fields on this page appear dimmed. However, if you previously entered information on this page, that information is retained so that you can easily re-enable e-mail notifications later. If you clear this option, you do not have to complete the rest of this procedure; simply click **Apply**.
4. In the **SMTP server name or IP address** text box, enter the fully qualified domain name or IP address of your e-mail server.
5. Specify where or not your e-mail server requires authentication by selecting or clearing the **SMTP server authentication** check box.

   If you select this option, you must enter a user name and password for logging into that server in the **User name** and **Password** text boxes. If you clear this op-

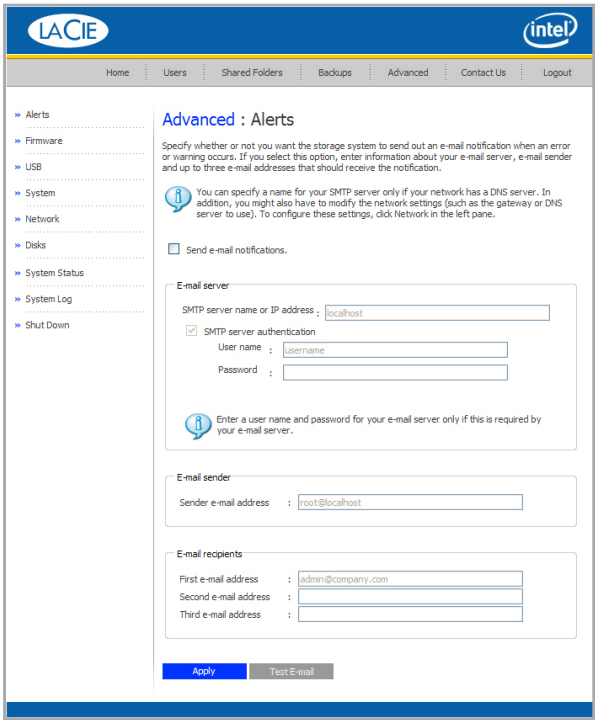

LACIE
intel
Home
Users
Shared Folders
Backups
Advanced
Contact Us
Logout
Alerts
Firmware
USB
System
Network
Disks
System Status
System Log
Shut Down
Advanced : Alerts
Specify whether or not you want the storage system to send out an e-mail notification when an error or warning occurs. If you select this option, enter information about your e-mail server, e-mail sender and up to three e-mail addresses that should receive the notification.
You can specify a name for your SMTP server only if your network has a DNS server. In addition, you might also have to modify the network settings (such as the gateway or DNS server to use). To configure these settings, click Network in the left pane.
Send e-mail notifications.
E-mail server
SMTP server name or IP address : localhost
SMTP server authentication
User name : username
Password :
Enter a user name and password for your e-mail server only if this is required by your e-mail server.
E-mail sender
Sender e-mail address : root@localhost
E-mail recipients
First e-mail address : admin@company.com
Second e-mail address :
Third e-mail address :
Apply
Test E-mail

Fig. 5.7.1.

IMPORTANT INFO: The e-mail might not be sent immediately when the problem occurs, but will be sent within five minutes of the event. In addition, if the problem is fixed within that time frame - for example, if you replace the disk that failed - the alert will not be sent.

tion, no authentication will be performed.

6. If your e-mail server cannot use the default sender e-mail address (root@localhost), or if you want the individuals who receive e-mail notifications to be able to reply to the alert, enter the address that you want to appear as the return address in the **Sender e-mail** address text box.

   For example, you could enter your own e-mail address (such as MyName@MyCompany.com).

7. In the **First e-mail address** text box, enter the e-mail address of an individual who should receive e-mail notifications when a problem occurs. The e-mail address can be up to 128 characters long and must include the @ symbol (for example, MyName@MyCompany.com).

8. If you want e-mail notifications to be sent to other individuals as well, enter the appropriate e-mail addresses in the **Second e-mail address** and **Third e-mail address** text boxes.

9. Click **Apply**.

10. When the confirmation message appears, click **OK**.

11. To confirm that the configuration is correct, click **Test E-mail**, and click **OK** on the confirmation message.

    This sends a test message to the specified recipients. If they do not receive the test message, make sure that all the entries on this page are correct. You might also have to modify the network settings (such as the gateway to use). For information about changing the network settings, refer to section 5.7.5. Network.

5.7.2. Firmware

The **Firmware** page displays the current version of the firmware that is installed on your Ethernet Disk RAID. It also allows you to upgrade it if newer firmware becomes available.

For additional security, you must enter your administrator password in order to upgrade the firmware.

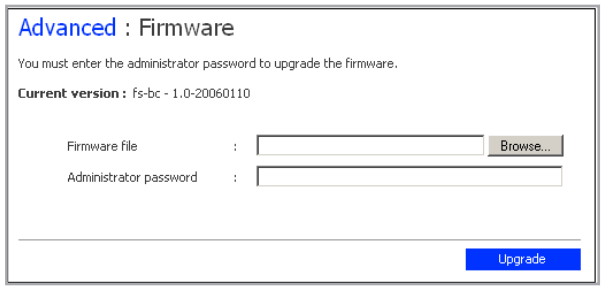


Fig. 5.7.2.

To upgrade the firmware:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Firmware**.
3. In the **Firmware file** text box, enter the path and file name for the firmware package (such as D:\fs20060921.pkg), or click **Browse** and select the file from the displayed list.
4. In the **Administrator password** text box, enter the password that you use for logging in to the Manager.
5. Click **Upgrade**.
6. When the confirmation message appears, click **OK**.

CAUTION: When you upgrade the firmware, the Ethernet Disk RAID restarts, and access to the Manager is temporarily interrupted. In addition, users will not be able to access the shared folders while the system restarts. If users have shared files open, data might be lost. Be sure to have all users save their changes and close any open files before you upgrade the firmware.

Restarting the Ethernet Disk RAID when a backup is occurring will not have any adverse effect; the backup will resume automatically when the Ethernet Disk RAID resumes operation. However, restarting when a disk is being recovered can potentially corrupt the user's operating system, and the user will have to recover the system disk using the recovery CD (or, if the system disk was not protected, re-install the operating system). Be sure to upgrade the firmware only when recovery is not occurring.

5.7.3. USB

The USB page displays a list of all USB devices that are currently attached to the Ethernet Disk RAID. USB disks are identified by the names usbdisk1 and usbdisk2. (These names cannot be changed.)

To unplug a USB device from the Ethernet Disk RAID, you must first use the Manager to disconnect it.

To disconnect a USB device:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **USB.**
3. In the list of USB devices, select the device(s) that you want to disconnect.
4. Click **Disconnect**.
5. When the confirmation message appears, click **OK**.

You can now unplug the USB device.

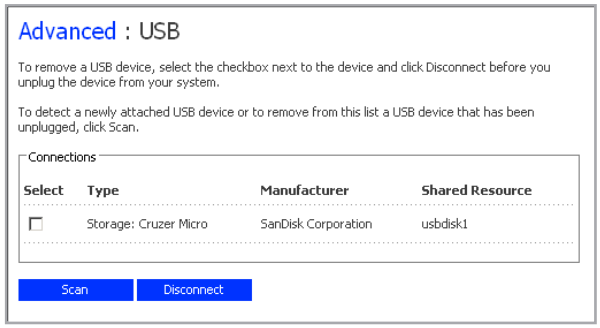

Advanced : USB
To remove a USB device, select the checkbox next to the device and click Disconnect before you unplug the device from your system.
To detect a newly attached USB device or to remove from this list a USB device that has been unplugged, click Scan.
Connections
Select
Type
Manufacturer
Shared Resource
Storage: Cruzer Micro
SanDisk Corporation
usbdisk1
Scan
Disconnect

Fig. 5.7.3.

TECHNICAL NOTE: If you inadvertently disconnect a USB device, unplug it from the Ethernet Disk RAID, plug it back in, and then click **Scan**. This reactivates the USB device. User assignments are always retained.

5.7.4. System

The **System** page displays the settings that you specified when you initially configured the Ethernet Disk RAID, such as the system name, and the current date and time.

Using the **System** page, you can also change the administrator name and password to use for logging in to the Manager, as well as the password to use for protecting local disks.

To change any of the system settings:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **System**.

(continued on next page)

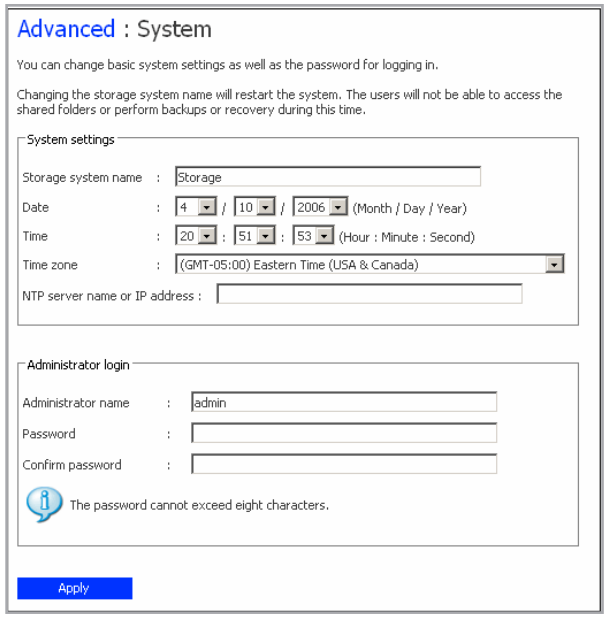

Advanced : System
You can change basic system settings as well as the password for logging in.
Changing the storage system name will restart the system. The users will not be able to access the shared folders or perform backups or recovery during this time.
System settings
Storage system name : Storage
Date : 4 / 10 / 2006 (Month / Day / Year)
Time : 20 : 51 : 53 (Hour : Minute : Second)
Time zone : (GMT-05:00) Eastern Time (USA & Canada)
NTP server name or IP address :
Administrator login
Administrator name : admin
Password :
Confirm password :
The password cannot exceed eight characters.
Apply

Fig. 5.7.4.

TECHNICAL NOTE: If you change the name of the system, be sure to also change that name in any local hosts files or on the DNS server in your network. The Ethernet Disk RAID does not register its name with your DNS server automatically.

3. Make the desired changes:

■ System Settings Options	
To change this	**Do this**
The system name	In the Storage system name text box, enter the new name to use for the Ethernet Disk RAID. This name can be up to 15 characters long and can include letters, numbers, and hyphens.
The system date, time, or time zone	❖ In the Date fields, enter or select the desired month, date, and year. ❖ In the Time field, enter or select the desired hour, minute, and second. ❖ In the Time zone list, select the desired time zone.
Network Time Protocol (NTP) server name or IP address	In the NTP server name or IP address text box, enter the name or IP address of the NTP server from which the storage system should set its time. The Ethernet Disk RAID will synchronize its time with the NTP server every hour. You can use a name only if it is resolvable.
The administrator name or password	In the Administrator name text box, enter the user name to use for logging in to the Manager. In the Password and Confirm password text boxes, enter the password to use for logging in to the Manager. The user name and password are case-sensitive.

4. Click **Apply**.
5. When the confirmation message appears, click **OK**.

5.7.5. Network

The **Network** page (Fig. 5.7.5) displays the network settings that were set when you initially configured the Ethernet Disk RAID. (Only the first Ethernet port was configured during setup. The second uses its default settings unless you change them here.) You can change these settings at any time.

You can also configure the Ethernet Disk RAID to act as a DHCP server. In other words, the system can assign IP addresses to other computers in your network, simplifying the network configuration of each individual system.

In addition, your Ethernet Disk RAID can act as an FTP server. This allows all Windows or Mac OS X users to use a Web browser to access the public folder. They can also access their personal folder that was created automatically when their user name was added (as described in section 5.4.1. Adding Users). For more information, refer to section 5.7.6. Reconfiguring the Disks.

TECHNICAL NOTE: Changing the IP address or subnet mask can have several effects:

- Access to the Manager will be temporarily disrupted. If you access the Manager using a Web browser and an IP address, you will need to use the new IP address. In addition, if you added the Ethernet Disk RAID's IP address to a local hosts file or DNS server, you must update the IP address in those resources.
- Users who accessed the shared folders using the previous IP address will be disconnected and must access them again using the new IP address (as described in section 6.1. Accessing Shared Folders).

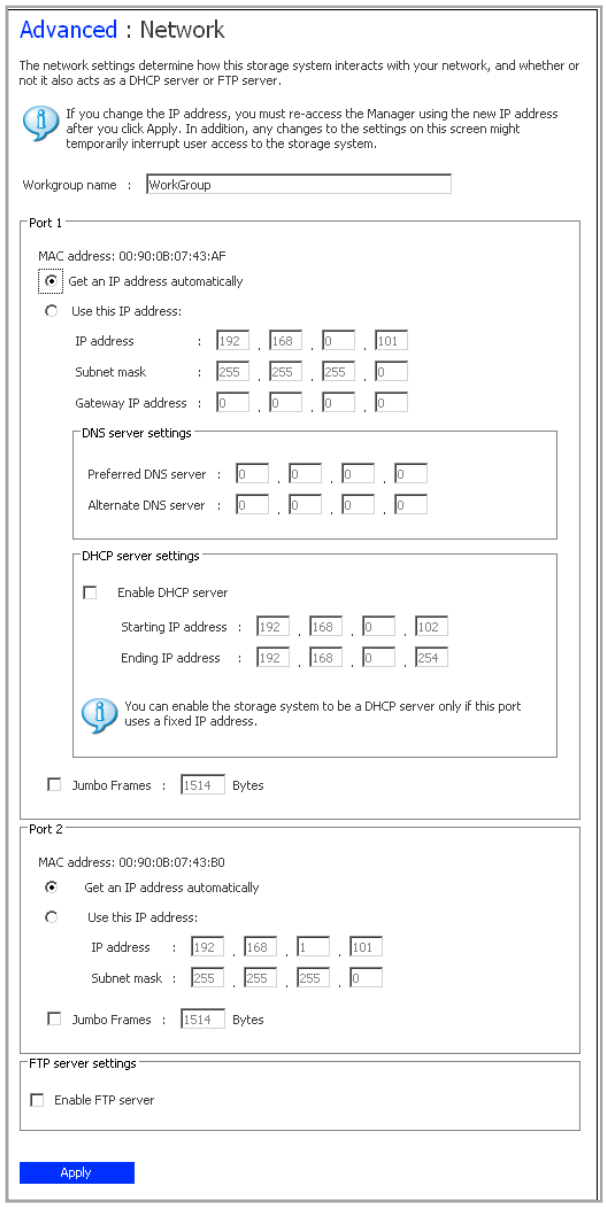

Advanced : Network
The network settings determine how this storage system interacts with your network, and whether or not it also acts as a DHCP server or FTP server.
If you change the IP address, you must re-access the Manager using the new IP address after you click Apply. In addition, any changes to the settings on this screen might temporarily interrupt user access to the storage system.
Workgroup name : WorkGroup
Port 1
MAC address: 00:90:0B:07:43:AF
Get an IP address automatically
Use this IP address:
IP address : 192 . 168 . 0 . 101
Subnet mask : 255 . 255 . 255 . 0
Gateway IP address : 0 . 0 . 0 . 0
DNS server settings
Preferred DNS server : 0 . 0 . 0 . 0
Alternate DNS server : 0 . 0 . 0 . 0
DHCP server settings
Enable DHCP server
Starting IP address : 192 . 168 . 0 . 102
Ending IP address : 192 . 168 . 0 . 254
You can enable the storage system to be a DHCP server only if this port uses a fixed IP address.
Jumbo Frames : 1514 Bytes
Port 2
MAC address: 00:90:0B:07:43:B0
Get an IP address automatically
Use this IP address:
IP address : 192 . 168 . 1 . 101
Subnet mask : 255 . 255 . 255 . 0
Jumbo Frames : 1514 Bytes
FTP server settings
Enable FTP server
Apply

Fig. 5.7.5.

To change any of the network settings:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Network**.
3. Make the desired changes:

■ Network Settings Options

To change this	Do this
The workgroup to which the Ethernet Disk RAID belongs	In the **Workgroup name** text box, enter the name of the workgroup. This name can be up to 15 characters long.
The IP address(es) used by the Ethernet Disk RAID	In the **Port 1** group box, either select **Get an IP address automatically** to obtain the IP address from your DHCP server, or select **Use this IP address** and enter the IP address and subnet mask in the subsequent text boxes. If you're using the second Ethernet port, do the same in the **Port 2** group box.
The IP address of the gateway	If your network includes a gateway, and if the first port on the Ethernet Disk RAID uses a specified IP address rather than obtaining one from the DHCP server, enter the IP address of the default router in the **Gateway IP address** text boxes. (This is typically the same IP address as the first port, with the last number being 1.) If your network does not include a gateway, or if the first port obtains its IP address from the DHCP server, leave these text boxes blank. (If the first port obtains its IP address from a DHCP server, the gateway will obtain its IP address from the DHCP server as well.)
The DNS server to use	If your network includes a DNS server, and if the first port on the Ethernet Disk RAID uses a specified IP address rather than obtaining one from the DHCP server, enter the primary IP address in the **Preferred DNS server** text boxes and the secondary IP address in the **Alternate DNS server** text boxes. If your network does not include a DNS server, or if the first port obtains its IP address from the DHCP server, leave these text boxes blank. (If the first port obtains its IP address from a DHCP server, the DNS server IP address will be obtained from the DHCP server as well.)

■ Network Settings Options

To change this	Do this
The IP address(es) used by the Ethernet Disk RAID	In the **Port 1** group box, either select Get an IP address automatically to obtain the IP address from your DHCP server, or select **Use this IP address** and enter the IP address and subnet mask in the subsequent text boxes. If your Ethernet Disk RAID has two Ethernet ports and you're using the second one, do the same in the **Port 2** group box. (This group box does not appear if your system supports only one Ethernet port.)
The DHCP settings	If you want to use the Ethernet Disk RAID as a DHCP server, in the **Port 1** group box, select **Use this IP address** and enter the IP address and subnet mask in the subsequent text boxes. Then select the **Enable DHCP server** check box, enter the beginning IP address in the **Starting IP address** text boxes, and enter the last IP address in the **Ending IP address** text boxes. For example, if the Starting IP address is 192.168.0.103 and the Ending IP address is 192.168.0.107, the Ethernet Disk RAID will allocate the IP addresses 192.168.0.103, 192.168.0.104, 192.168.0.105, 192.168.0.106, and 192.168.0.107 to the first five computers that try to obtain their IP addresses from the Ethernet Disk RAID. As soon as one of those computers shuts down or otherwise loses its network connection, that IP address will be assigned to the next computer that tries to obtain its IP address from the Ethernet Disk RAID. If you do not want to use the Ethernet Disk RAID as a DHCP server, clear the **Enable DHCP server** check box. (If **Get an IP address** automatically is selected, you cannot use the Ethernet Disk RAID as a DHCP server.)

■ Network Settings Options

To change this	Do this
The packet size for transferring data	Specify whether or not to transfer larger data packets between the Ethernet Disk RAID and the computers in your network by selecting or clearing the **Jumbo Frames** check box. If you clear this option, the Ethernet Disk RAID will use 1514-byte packets. If you select this option, you can specify a larger packet size (from 1514 to 9014 bytes). **TECHNICAL NOTE:** Using jumbo frames allows you to transfer data more quickly. However, you can select this option only if your network, Ethernet switch, and the network interface cards (NICs) on the computers in your network support the specified packet size. To determine whether you can use jumbo frames, refer to the documentation for those components.
The FTP settings	If you want to use the Ethernet Disk RAID as an FTP server, select the **Enable FTP server** check box. If you do not want to use it as an FTP server, clear this option. For information about accessing the Ethernet Disk RAID using FTP, refer to section 5.2. Accessing Shared Folders Using FTP.

4. Click **Apply**.
5. When the confirmation message appears, click **OK**.

TECHNICAL NOTE: If you changed the IP address of the Ethernet Disk RAID, you must now access the Manager using the new IP address.

5.7.6. Reconfiguring the Disks

The **Disks** page displays information about all the hard disks that are currently installed in your Ethernet Disk RAID.

This page includes the following details:

- The disk configuration (that is, whether the disks use a linear or RAID configuration,

  and the RAID level)
- The overall status of the disks:
  - Normal – All the disks are working properly.
  - Degraded – One or more disks have failed but all the data is still available.
  - Failed – The Ethernet Disk RAID has stopped working properly.
- The slot where each hard disk resides
- The model number, serial number, and size of each hard disk
- The current status of each disk:
  - Linear or RAID *n* – The disk is working properly as part of the specified configuration.
  - New – The disk has been added to the Ethernet Disk RAID but is not currently being used.
  - Spare – The disk is acting as a spare disk for the RAID.
  - Rebuilding – The disk is being rebuilt (for example, when a failed disk is replaced)
  - N/A – The disk is detected but not available for use (for example, when it has failed)
- The hot-plug indicator:
  - RED – Removing the disk will cause the RAID to fail.
  - YELLOW – Removing the disk will cause RAID degradation.
  - GREEN – Removing the disk will not affect the RAID.

TECHNICAL NOTE: Whenever you add or remove a disk from the Ethernet Disk RAID, you must click Refresh to update the hot-plug indicator.

IMPORTANT INFO: For detailed information about RAIDs and how adding, removing, or swapping disks affects the Ethernet Disk RAID, refer to section 11. RAID and Storage Policies.

You can change the disk configuration or amount of storage space that is allocated for shared folders at any time. However, for additional security, you must enter your administrator password to be able to make these changes.

5.7.6.1. Expanding the Shared Storage

The disk space on your Ethernet Disk RAID is divided into two portions. One portion is for shared folders; the other is for backups of your computer disks. The Storage Status view on the Home page shows how much disk space is currently allocated for shared folders, how much is used by backups, and how much is available for either.

You can expand the amount of disk space allocated for shared folders (as long as free disk space is available), but you cannot reduce it without reconfiguring your disks and losing all your data. Therefore, it is recommended that you allocate the least amount of space for shared folders until all the computer disks that you plan to protect have been backed up.

To expand the amount of disk space allocated for shared folders:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Disks**.
3. In the **Administrator password** text box, enter your password for logging in to the Manager.
4. Click **Expand Shared Storage**.

   The **Expand Shared Storage** page appears (see Fig. 4.10).
5. Specify how much disk space to add to the space that is currently allocated for shared folders.

   To allocate all available disk space, select **Add all available disk space**.

   To allocate a specific amount, select **Add this much disk space** and enter the desired number of gigabytes. (The minimum is 1 GB, and the maximum is the total amount of space currently available. You can specify only whole numbers.)
6. Click **OK**.
7. When the confirmation message appears, click **OK**.

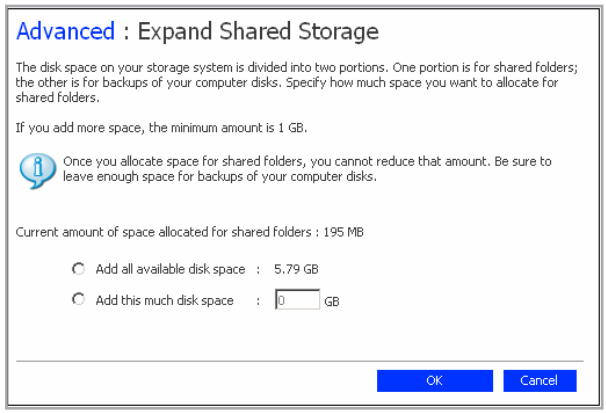

Advanced : Expand Shared Storage
The disk space on your storage system is divided into two portions. One portion is for shared folders; the other is for backups of your computer disks. Specify how much space you want to allocate for shared folders.
If you add more space, the minimum amount is 1 GB.
Once you allocate space for shared folders, you cannot reduce that amount. Be sure to leave enough space for backups of your computer disks.
Current amount of space allocated for shared folders : 195 MB
Add all available disk space : 5.79 GB
Add this much disk space : 0 GB
OK
Cancel

Fig. 5.7.6.1.

5.7.6.2. Reconfiguring the Disks

CAUTION: Changing the disk configuration will delete all user information and all data on all the disks.

Before you do this, have all the users disconnect from all shared folders (as described in section 5.3. Disconnecting from Shared Folders Using FTP) and remove protection from all disks (as described in section 7.9.5. Removing Protection).

When you are done, you must re-add all users (as described in section 4.1.1. Adding Users), create new shared folders (as described in section 5.5.1. Creating Shared Folders), and have all users once again access the shared folders (as described in section 6.1. Accessing Shared Folders) and protect their disks (as described in section 7.2. Protecting Your Disks).

To change the disk configuration:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Disks**.
3. In the **Administrator password** text box, enter your password for logging in to the Manager.
4. Click **Reconfigure Disks**.
5. When the confirmation message appears, click **OK**.

The **Disk Configuration** page appears (see Fig. 5.7.6.2.A.). The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.

If you want to add or remove hard disks, do so one at a time and click **Scan** after each action. If you're adding disks, wait until the disk LED is green before you click **Scan**. To accept the default disk configuration (which will provide the best level of data protection available for the number of hard disks currently installed), click **Next**. By default, a linear disk

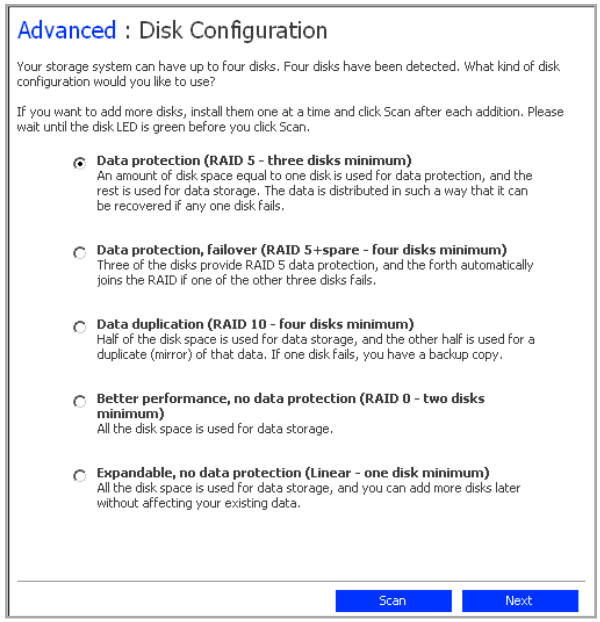

Advanced : Disk Configuration
Your storage system can have up to four disks. Four disks have been detected. What kind of disk configuration would you like to use?
If you want to add more disks, install them one at a time and click Scan after each addition. Please wait until the disk LED is green before you click Scan.
Data protection (RAID 5 - three disks minimum)
An amount of disk space equal to one disk is used for data protection, and the rest is used for data storage. The data is distributed in such a way that it can be recovered if any one disk fails.
Data protection, failover (RAID 5+spare - four disks minimum)
Three of the disks provide RAID 5 data protection, and the forth automatically joins the RAID if one of the other three disks fails.
Data duplication (RAID 10 - four disks minimum)
Half of the disk space is used for data storage, and the other half is used for a duplicate (mirror) of that data. If one disk fails, you have a backup copy.
Better performance, no data protection (RAID 0 - two disks minimum)
All the disk space is used for data storage.
Expandable, no data protection (Linear - one disk minimum)
All the disk space is used for data storage, and you can add more disks later without affecting your existing data.
Scan
Next

Fig. 5.7.6.2.A.

configuration is used for a single hard disk, RAID 1 is used for two hard disks, and RAID 5 is used for three or four hard disks.

If you want to change the disk configuration, select the desired RAID level and then click **Next**. (For detailed information about the different RAID levels, refer to Section 11. Raid and Storage Policies) The **Disk Space Distribution** page appears (see Fig. 5.7.6.2.B).

6. To accept how the disk space will be proportioned for shared folders and backups (only 200 MB will be allocated for shared folders), click **Finish**.

   If you want to allocate more space for shared folders, select **Allocate more space** for shared folders and then specify how much space to allocate (either **All available disk space** or **Specified disk space**). If you select **Specified disk space**, enter the number of gigabytes to allocate for shared folders (the minimum is 1 GB). Then click **Finish**.

7. When the confirmation message appears, click **OK**. The screen displays the progress of the process (see Fig. 5.7.6.2.C and 5.7.6.2.D). When this process is complete, the Ethernet Disk RAID restarts.

   Close the browser window. After the system has restarted, you can access the Manager and re-create your users and shared folders (as described in section 5.4.1. Adding Users and section 5.5.1. Creating Shared Folders).

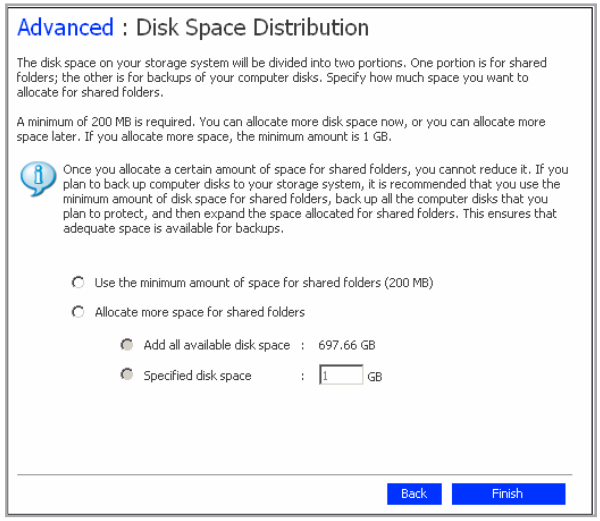

Advanced : Disk Space Distribution
The disk space on your storage system will be divided into two portions. One portion is for shared folders; the other is for backups of your computer disks. Specify how much space you want to allocate for shared folders.
A minimum of 200 MB is required. You can allocate more disk space now, or you can allocate more space later. If you allocate more space, the minimum amount is 1 GB.
Once you allocate a certain amount of space for shared folders, you cannot reduce it. If you plan to back up computer disks to your storage system, it is recommended that you use the minimum amount of disk space for shared folders, back up all the computer disks that you plan to protect, and then expand the space allocated for shared folders. This ensures that adequate space is available for backups.
Use the minimum amount of space for shared folders (200 MB)
Allocate more space for shared folders
Add all available disk space : 697.66 GB
Specified disk space : 1 GB
Back
Finish

Fig. 5.7.6.2.B

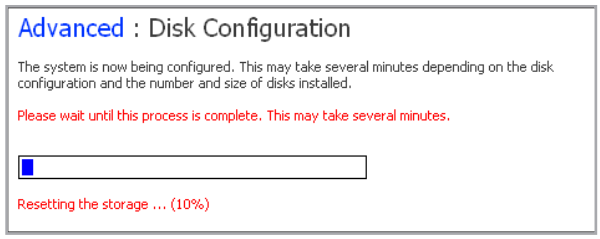

Advanced : Disk Configuration
The system is now being configured. This may take several minutes depending on the disk configuration and the number and size of disks installed.
Please wait until this process is complete. This may take several minutes.
Resetting the storage ... (10%)

Fig. 5.7.6.2.C

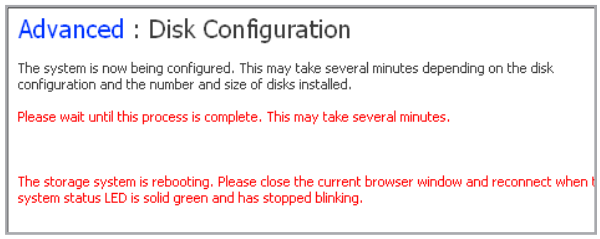

Advanced : Disk Configuration
The system is now being configured. This may take several minutes depending on the disk configuration and the number and size of disks installed.
Please wait until this process is complete. This may take several minutes.
The storage system is rebooting. Please close the current browser window and reconnect when
system status LED is solid green and has stopped blinking.

Fig. 5.7.6.2.D

TECHNICAL NOTE: You can expand the amount of disk space allocated for shared folders later (as long as free disk space is available), but you cannot reduce it without reconfiguring your disks and losing all your data.

If you plan to back up computer disks to your Ethernet Disk RAID, it is recommended that you use the minimum amount of space for shared folders, back up all the computer disks that you plan to protect, and then expand the space allocated for shared folders. This ensures that adequate space is available for backups.

5.7.7. System Status

When you click **Advanced** in the navigation bar and click **System Status** in the left pane, you can view many of the operational parameters of your Ethernet Disk RAID, including CPU usage, memory usage, the amount of time that the Ethernet Disk RAID has been running, the current fan speed, the temperatures of the CPU and disks, the IP address of the gateway (which you can change as described in section 5.7.5. Network), the IP address(es) of the DNS servers in your network, the network settings of your ports (several of which you can change as described in section 5.7.5. Network), the MAC addresses of your ports, and the speed at which data is being sent and received.

To update the information on this page, click **Refresh**.

TECHNICAL NOTE: The fan speed changes depending on the temperature of the unit. If the temperature of the CPU reaches or exceeds 85° C (185° F), or if the temperature of any of the disks reaches or exceeds 55° C (131° F), the Ethernet Disk RAID shuts down automatically.

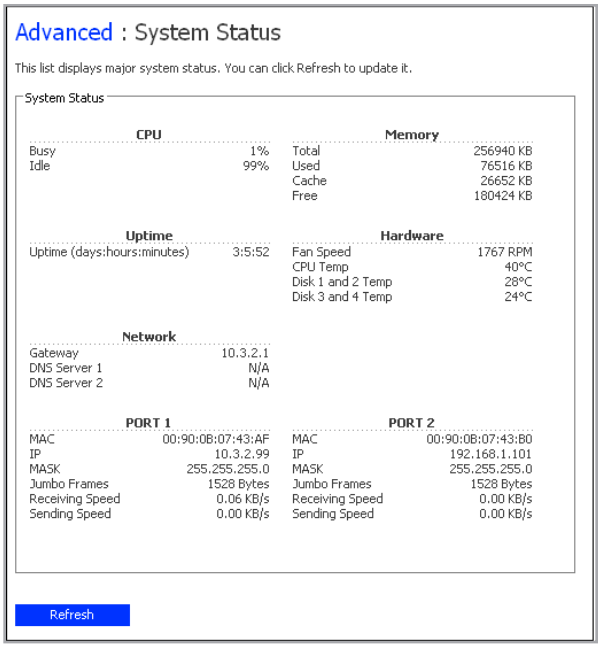


Fig. 5.7.7.

5.7.8. System Log

The **System Log** page displays a list of events that have occurred on the Ethernet Disk RAID. Reviewing this list can help you identify and resolve any problems that you might encounter.

To view event information:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **System Log**.

   The System Log page displays the date and time of the event, the type of event (I for Informational, E for error, W for warning, and C for critical), and a brief description of the event.
3. If an event occurs while you're viewing this list, click **Refresh** to update it.

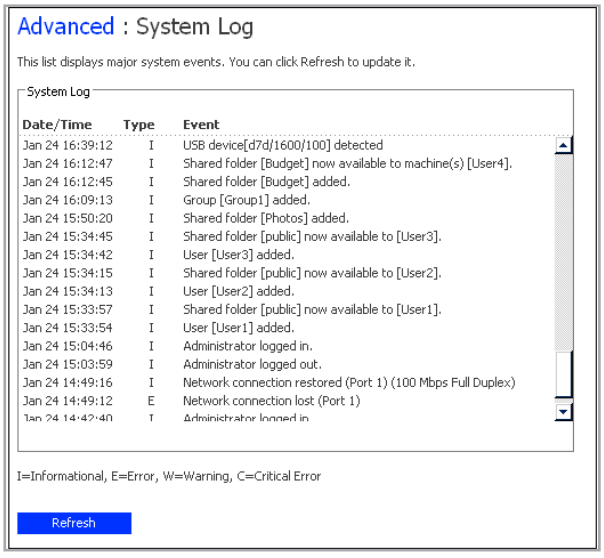

Advanced : System Log
This list displays major system events. You can click Refresh to update it.
System Log
Date/Time Type Event
Jan 24 16:39:12 I USB device[d7d/1600/100] detected
Jan 24 16:12:47 I Shared folder [Budget] now available to machine(s) [User4].
Jan 24 16:12:45 I Shared folder [Budget] added.
Jan 24 16:09:13 I Group [Group1] added.
Jan 24 15:50:20 I Shared folder [Photos] added.
Jan 24 15:34:45 I Shared folder [public] now available to [User3].
Jan 24 15:34:42 I User [User3] added.
Jan 24 15:34:15 I Shared folder [public] now available to [User2].
Jan 24 15:34:13 I User [User2] added.
Jan 24 15:33:57 I Shared folder [public] now available to [User1].
Jan 24 15:33:54 I User [User1] added.
Jan 24 15:04:46 I Administrator logged in.
Jan 24 15:03:59 I Administrator logged out.
Jan 24 14:49:16 I Network connection restored (Port 1) (100 Mbps Full Duplex)
Jan 24 14:49:12 E Network connection lost (Port 1)
I=Informational, E=Error, W=Warning, C=Critical Error
Refresh

Fig. 5.7.8.

5.7.9. Shut Down

To shut down the Ethernet Disk RAID, you can press the power button on the unit itself, or you can shut the system down remotely using the Manager.

To shut down the Ethernet Disk RAID using the Manager:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Shut Down**.
3. In the Administrator password text box, enter the password "Manager."
4. Click **Shut Down**.

A message appears, indicating that the system is shutting down.

Once the Ethernet Disk RAID shuts down, if you refresh the browser window, it will be blank. If you subsequently try to access the Manager, an error message will appear, since the Ethernet Disk RAID will no longer be running.

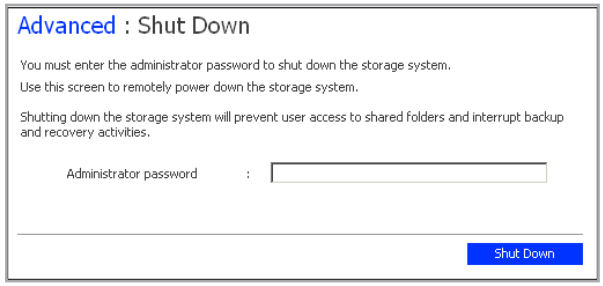

Advanced : Shut Down
You must enter the administrator password to shut down the storage system.
Use this screen to remotely power down the storage system.
Shutting down the storage system will prevent user access to shared folders and interrupt backup and recovery activities.
Administrator password :
Shut Down

Fig. 5.7.9.

CAUTION: If you shut down the Ethernet Disk RAID, users will no longer be able to access the shared folders. If users have shared files open, data might be lost. Be sure to have all users save their changes and close any open files before you shut down.

Shutting down the Ethernet Disk RAID when a backup is occurring will not have any adverse effect; the backup will resume automatically when the storage server is powered on again. However, shutting down when a disk is being recovered can potentially corrupt the user's operating system, and the user will have to recover the system disk using the recovery CD (or, if the system disk was not protected, re-install the operating system).

5.8. Logging Out of the Manager

It is recommended that you log out when not using the manager to ensure that unauthorized individuals do not make changes to the Ethernet Disk RAID.

To log out:

1. In the navigation bar, click **Log Out**.
2. When the confirmation message appears, click **OK**. The **Log Out** page appears (see Fig. 5.8.).
3. To log back in to the Manager later, click **Log In**.

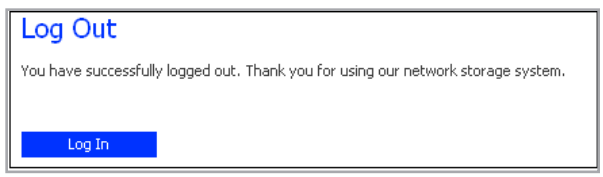


Fig. 5.8.

6. Working With Shared Folders

6.1. Accessing Shared Folders

Once you have added users and created shared folders (as described in section 5.4.1. Adding Users and section 5.5.1. Creating Shared Folders), the users need to perform some simple steps to be able to access those folders. The procedure for doing this varies, depending on the user's operating system. Each user can access only those shared folders that the user is authorized to access.

IMPORTANT INFO: If you change the IP address of the Ethernet Disk RAID, users who accessed the shared folders using the previous IP address will be disconnected and must repeat the procedures described here using the new IP address.

6.1.1. Windows Users

If you're using Microsoft Windows*, you have two options for accessing shared folders: you can use My Computer or Windows Explorer to map a drive letter to the shared folder, or you can install the Console and use that utility to map a drive letter to the shared folder. With the Console, you don't have to worry about remembering the name of the storage server or the shared folders; it displays them automatically. However, the computer where you install the Console must be on the same subnet as the Ethernet Disk RAID.

6.1.1.1. Using My Computer or Windows Explorer

To access a shared folder using My Computer or Windows Explorer:

1. Open **My Computer** or **Windows Explorer**.
2. From the **Tools** menu, click **Map Network Drive**. The Map Network Drive dialog box appears (see Fig. 6.1.1.1.).

   The exact appearance of this dialog box varies, depending on your operating system.
3. In the **Drive** list, select the drive letter that you want to assign to the shared folder.
4. In the **Folder** text box, enter the following:

   \\storage_system\shared_folder

   where storage_system is the name or IP address of the Ethernet Disk RAID and shared_folder is the name of the shared folder. For example, if your Ethernet Disk RAID's IP address is 192.168.0.101 and the shared folder name is Photos, you would enter the following:

   \\192.168.0.101\Photos

   Alternatively, you can click **Browse** and select the shared folder from the Microsoft Windows Network.
5. To automatically connect to this shared folder each time you log on to Windows, select **Reconnect at logon**.

   If you clear this option, you must repeat this procedure each time you want to access the shared folder.
6. Click **Finish**.
7. If prompted, enter your user name and password for accessing this shared folder, and then click **OK**.

   If the guest user has access to this shared folder, you can use guest as both the user name and password.

   You can now access the shared folder from My Computer or Windows Explorer.

Map Network Drive
Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Z:
Folder:
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel

Fig. 6.1.1.1.

TECHNICAL NOTE: If you connect a Ethernet Disk RAID to the network after the Console has already scanned it, or if you change the IP address of the Ethernet Disk RAID, you must click Discover Storage Systems to scan the network again and update the tree in the left pane.

TECHNICAL NOTE: If the user name and password for accessing the shared folder are the same as your Windows user name and password, you are not prompted to provide a user name and password to access the shared folder.

In addition, once you provide your user name and password for accessing one shared folder, you are not prompted to provide it again when you access other shared folders to which you have access rights.

6.1.1.2. Using the Console

To access a shared folder using the Console:

1. Install the Console (as described in section 3.2.1. Installing the Console).
2. Click **Start** ➔ **Programs** ➔ **Storage System Console**. The Console application window appears (see Fig. 6.1.1.2.A).

As soon as you start the Console, it automatically scans the network for storage devices. This might take a few minutes. As soon as the scan is complete, the left pane displays a tree view of all the storage devices it found (see Fig. 6.1.1.2.B).

Each Ethernet Disk RAID has two ports for connecting to the network. If your Ethernet Disk RAID uses both ports, two items appear in the tree in the left pane, each using the same name. You can identify the IP address used by each port by clicking each item in the tree and observing the IP address area in the right pane.

TECHNICAL NOTE: If you connect an Ethernet Disk RAID to the network after the Console has already scanned it, or if you change the IP address of the Ethernet Disk RAID, you must click **Discover Storage Systems** to scan the network again and update the tree in the left pane.

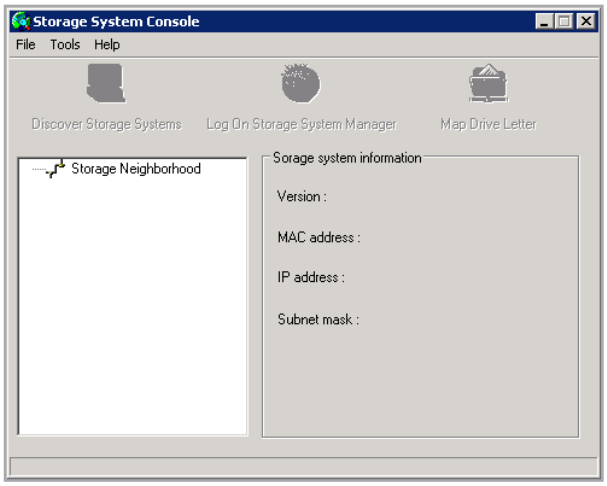


Fig. 6.1.1.2.A

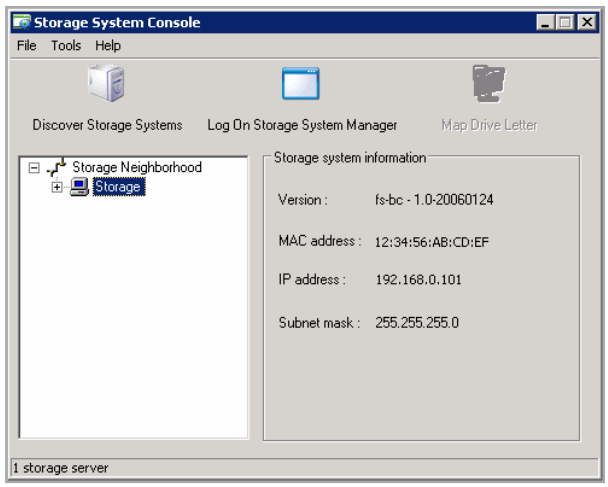


Fig. 6.1.1.2.B

3. In the left pane, double-click the name of the Ethernet Disk RAID that contains the shared folders that you want to access.

   If your Ethernet Disk RAID uses both available ports to connect to the network, you can double-click either name.

   The system name expands to display all the available shared folders. Those shared folders that can be accessed using the guest user name and password are listed first. See Fig. 6.1.1.2.C.

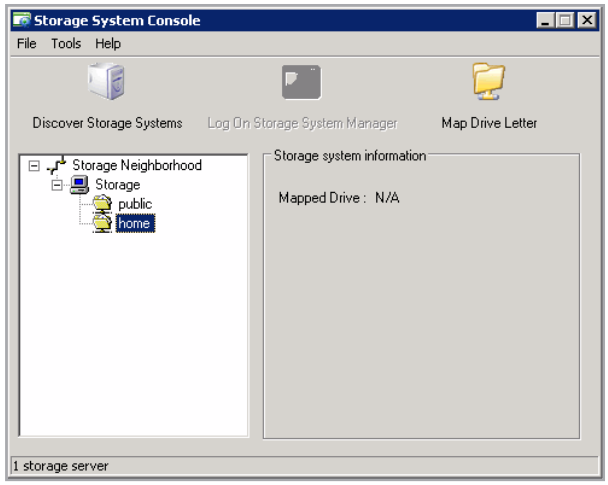


Fig. 6.1.1.2.C

4. In the left pane, select the name of the shared folder that you want to access (for example, home), and then click **Map Drive Letter**. To access a folder other than home, you must log in as a user with access to that folder.

   The **Map Network Drive** dialog box appears with the name of the folder installed (see Fig. 6.1.1.2.D).

   The exact appearance of this dialog box varies, depending on your operating system.

5. In the **Drive** list, select the drive letter that you want to assign to the shared folder.

6. To automatically connect to this shared folder each time you log on to Windows, select **Reconnect** at logon.

   If you clear this option, you must repeat this procedure each time you want to access the shared folder.

7. Click **Finish**.

8. If prompted, enter your user name and password for accessing this shared folder, and then click **OK**.

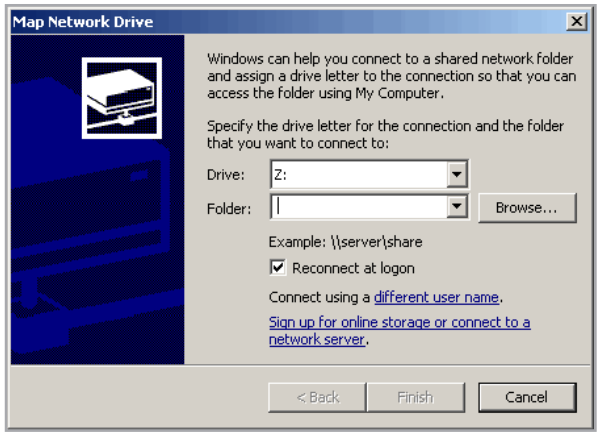

Map Network Drive
Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.
Specify the drive letter for the connection and the folder that you want to connect to:
Drive: Z:
Folder:
Browse...
Example: \\server\share
Reconnect at logon
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel

Fig. 6.1.1.2.D

TECHNICAL NOTE: If the user name and password for accessing the shared folder are the same as your Windows user name and password, you are not prompted to provide a user name and password to access the shared folder. In addition, once you provide your user name and password for accessing one shared folder, you are not prompted to provide it again when you access other shared folders to which you have access rights.

6.1.2. Linux Users

6.1.2.1. Using NFS

To access a shared folder on a computer running Linux:

1. Create a directory by entering the following command at the command prompt:

   mkdir /my_directory

   where my_directory is the name of the directory.

   Be sure to include the full path to the directory (for example, /mnt/my_directory).

2. If desired, display a list of all the available shared folders by entering the following

   command:

   showmount -e storage_system

   where storage_system is the IP address of the Ethernet Disk RAID.

3. Mount the desired shared folder by entering the following command:

   mount storage_system:/nas/NASDisk-00002/folder /mnt/my_directory

   where storage_system is the IP address of the Ethernet Disk RAID, folder is the shared folder, and my_directory is the name of the directory that you created step 1.

   If you included a full path when creating the directory, be sure to include the with this command, for example:

   mount storage_system:/nas/NASDisk-00002/folder /mnt/my_directory

4. Repeat steps 1 through 3 for each shared folder that you want to access.

6.1.2.2. Using SMBFS

On Linux, the SMBFS file system along with smbmount and smbclient tools can be used to mount remote samba shares onto a local Linux file system. Most of the Linux distributions include SMBFS support by default.

1. Create a directory by entering the following command at the command prompt:

   # mkdir /my_directory

   where my_directory is the name of the directory. Be sure to include the full path to the directory (for example, /mnt/my_directory).

2. If desired, display a list of all the available shares (and services) by entering the following command:

   # smbclient -L storage_system -U guest

   where Hostname is “storage_system” and Username is “guest”

3. Mount the desired shared folder by entering the following command:

   # smbmount //storage_system/share /my_directory -o username=guest

   where Hostname is “storage_system”, Username is “guest” and the sharename is “share” (as shown is the above listing)

4. Repeat steps 1 through 3 for each shared folder that you want to access.

5. Unmount the share directory

   # smbumount /my_directory

6.1.3. Mac Users

The procedure for accessing a shared folder on a Mac varies, depending on whether the Mac is running OS X or an older operating system. (Macs running OS X can access the same shared CIFS folders as Windows users. Macs running older operating systems can access the same shared NFS folders as Linux users.)

6.1.3.1. Mac OS X

To access a shared folder on a Mac running OS X:

1. From the **Go** menu, click **Connect to Server**.
2. In the **Address** text box, enter the following and click **Connect**:

   smb://storage_system

   where storage_system is either the name or IP address of the Ethernet Disk RAID
3. In the **Select a share** list, select the name of the shared folder that you want to access and then click **OK**.
4. Enter the user name and password for accessing this shared folder, and then click **OK**.

   If the guest user has access to this shared folder, you can use guest as both the user name and password.

   An icon with the name of the shared folder is created on the desktop.
5. Repeat steps 1 through 4 for each shared folder that you want to access.
6. To access the shared folder, double-click the icon on the desktop.

TECHNICAL NOTE: You can use the system name only if your computer is in the same subnet as the Ethernet Disk RAID, if you added the Ethernet Disk RAID's IP address and name to your local hosts file, or if you manually registered the name with a DNS server in your network.

6.1.3.2. Other Mac Operating Systems

For information about accessing a shared folder using NFS on a Mac running an operating system older than OS X, please refer to your Mac documentation.

6.2. Accessing Shared Folders Using FTP

If you enabled the Ethernet Disk RAID to act as an FTP server (as described in section 5.7.5. Network), all Windows and Mac OS X users can use a Web browser to access the public folder. They can also access their personal folder that was created automatically when their user name was added by logging in with their user name and password (as described in section 5.4.1. Adding Users). Anonymous FTP is not supported. They can use "guest" as the user name and password, but they will only be able to access the public folder.

TECHNICAL NOTE: Even if you changed the access rights to the public folder (for example, to prevent a particular user from accessing it altogether or to limit a user to read-only access), all existing users have full read/write access to the public folder when accessing it via FTP.

To access shared folders using FTP:

1. At any Windows or Mac OS X computer, open a Web browser, enter the following in the address bar, and press **Enter**:

   ftp://user_name@storage_system

   where user_name is the user name as defined on the Ethernet Disk RAID and storage_system is the name or IP address of the Ethernet Disk RAID (for example, ftp://user1@storage or ftp://user1@192.168.0.101).

   You can use guest as the user name, but you will be able to access only the public folder.

2. If prompted, enter your user name and password for accessing shared folders, and then click **OK**.

   If you used the guest user name, the password is also guest.

3. Double-click any of the displayed folders or files to open them.

   You have full read/write access to all the folders and files in both the public folder and your personal folder, and you can create new ones.

   Even if you browse to other websites, you remain logged in until you close the browser window. (That is, you can return to the FTP site using the **Back** button in your browser window.)

TECHNICAL NOTE: You can use the system name only if your computer is in the same subnet as the Ethernet Disk RAID, if you added the Ethernet Disk RAID's IP address and name to your local hosts file, or if you manually registered the name with a DNS server in your network.

TECHNICAL NOTE: Files copied to or from the Ethernet Disk RAID using FTP can be no larger than 2 GB.

6.3. Disconnecting from Shared Folders

If you need to reconfigure the disks in your Ethernet Disk RAID or shut it down for any reason, all users should disconnect from the shared folders to ensure that the process proceeds smoothly. You might also want to have users disconnect from the shared folders if you want to change their access rights, since otherwise the change will not take effect until the user shuts down the computer.

The procedure for disconnecting from a shared folder varies, depending on the operating system used by the user. (Users who connected to shared folders using FTP can disconnect simply by closing the browser window.)

6.3.1. Windows Users

If you are using Microsoft Windows, you have two options for accessing shared folders: you can use My Computer or Windows Explorer to map a drive letter to the shared folder, or you can install the Console and use that utility to map a drive letter to the shared folder. With the Console, you don't have to worry about remembering the name of the storage server or the shared folders; it displays them automatically. However, the computer where you install the Console must be on the same subnet as the Ethernet Disk RAID.

6.3.1.1. Using My Computer or Windows Explorer

1. Close any files that you currently have open in the shared folder.
2. In My Computer or Windows Explorer, right-click the drive for the shared folder and then click **Disconnect** from the pop-up menu.

   The shared folder no longer appears in My Computer or Windows Explorer.

6.3.1.2. Using the Console

1. Close any files that you currently have open in the shared folder.
2. Start the Console (as described in section 3.2.2. Starting the Console).
3. In the left pane, double-click the name of the Ethernet Disk RAID that contains the shared folder from which you want to disconnect.

   If your Ethernet Disk RAID uses both available ports to connect to the network, you can double-click either name. The name expands to display all the available shared folders.
4. In the left pane, select the name of the shared folder from which you want to disconnect, and then click **Unmap Drive Letter**.

   The shared folder no longer appears in My Computer or Windows Explorer.

6.3.2. Linux Users

Unmount the desired shared folder by entering the following command:

umount /my_directory

where my_directory is the name of the local directory.

For example, if you mounted the shared folder using the following command:

mount 192.168.0.101:/nas/NASDisk-00002/public /my_directory you would unmount it using the following command:

umount /my_directory

If you included an absolute path when mounting the shared folder (such as /mnt/my_directory), use the same path when unmounting it.

6.3.3. Mac OS X Users

1. On the desktop, select the shared folder from which you want to disconnect.
2. From the **File** menu, click **Eject**.

   Any open window to the shared folder closes, and the shared folder disappears from the desktop.

6.3.4. Other Mac Users

For information about disconnecting from a shared folder on a Mac running an operating system older than OS X, please refer to your Mac documentation.

7. Protecting Local Disks

Even if most of your data is stored and protected on your Ethernet Disk RAID, your operating system files, applications, and many other files still reside on each individual computer in your network. If one of those local disks fails, it can take many hours to re-install and reconfigure the operating system and applications on a new or repaired hard disk, and some files might be completely lost.

Windows Backup Software is a software application designed to address this issue. On each computer where it is installed, Windows Backup Software provides reliable data protection and rapid data recovery in the event of a system crash or disk failure.

Windows Backup Software protects Windows desktops and laptops by backing up their local disks or partitions. To make sure that you have recent copies of your local disk, Windows Backup Software can automatically perform a backup at regularly scheduled intervals—either once a day or once a week, whichever you prefer. (You can also disable automatic backups and just perform backups manually at a time of your choosing.) Once the maximum number of supported backups are saved on the Ethernet Disk RAID, the oldest backup is automatically deleted each time a new backup is performed.

To ensure that valuable storage space isn't used up by duplicate data, when Windows Backup Software performs each subsequent backup, it copies only the data that has changed since the last time a backup was performed. This also minimized the impact on your network. Yet through unique technology on the Ethernet Disk RAID, each backup is a complete point-in-time image. You can view or recover the entire disk or partition exactly as it existed at a particular date and time.

Whenever you want to recover data from the Ethernet Disk RAID, you can do so quickly and easily. If you need to recover just a few files or folders, you can access the desired backup and copy what you need back

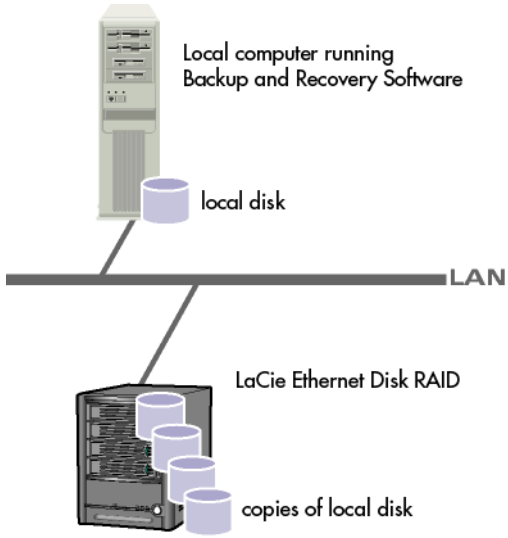


Fig. 7.

to your local disk. If you need to recover an entire data disk or partition (that is, a disk or partition that does not contain any of the files needed to run the operating system), you can do so using Windows Backup Software. And if you need to recover your whole system disk, you can do so using the recovery CD. (Alternately, if your computer does not support the recovery CD but does support the PXE protocol, you can boot your computer from a backup on the Ethernet Disk RAID and recover your system disk.) When you recover a disk, it contains exactly the same data that it contained at the time the backup was performed—you don't have to reinstall or reconfigure the operating system or applications.

7.1. Getting Started

7.1.1. System Requirements

Each computer where Windows Backup Software is installed must have the following:

Windows Users

- Microsoft Windows XP Home Edition or Professional (with or without Service Pack 1 or Service Pack 2), Microsoft Windows Server 2003, Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 4
- An enabled network interface card.
- A CD-ROM drive (for installation and using the recovery CD).
- Microsoft iSCSI Initiator*2.x
- 20 MB free hard disk space

TECHNICAL NOTE: A CD-ROM drive is not required for installation if an image of the CD is accessible via a network server.

IMPORTANT INFO: For information about downloading and installing this item, refer to the next section, "Installing the Microsoft iSCSI Initiator."

IMPORTANT INFO: Windows Backup Software requires the Intelligent Management Agent (IMA), which is installed automatically if it is not already installed.

IMA requires an additional 5 MB of free hard disk space (for both the application and associated log file data).

The Microsoft .NET* Framework 1.1 is also required and installed automatically if it is not already installed. The .NET Framework requires approximately 40 MB of additional free hard disk space.

7.1.2. Additional Requirements

In addition to the system requirements, the following criteria must be met:

- You must be logged on as an administrator to install Windows Backup Software and run it for the first time. However, after you have run the application once as an administrator, you can subsequently run it when logged on as a user.
- If your computer name includes any characters other than letters (A-Z or a-z), numbers (0-9), hyphens (-), colons (:), or periods (.), you must change the computer name before you use Windows Backup Software to protect a disk.
- If you're using a firewall on the computer that you plan to protect, open TCP port 11762 on the firewall. This ensures that Windows Backup Software can communicate with the Ethernet Disk RAID. In additon, make sure that your firewall does not block incoming network communication to the Microsoft iSCSI Initiator*.

IMPORTANT INFO: Previous releases allowed the use of underscores (_) in the computer name. If your computer name included this character and you protected a disk, you must remove protection from all disks (as described in section 7.9.5. Removing Protection), delete the client (as described in section 5.6.4. Deleting a Client), and protect the disks again (as described in section 7.2. Protecting Your Disks). In addition, when you protect your disks again, you must remove the Ethernet Disk RAID from the list of backup locations and add it again (as described in step 4 in section 7.2. Protecting Your Disks.)

7.1.3. Installing the Microsoft iSCSI Initiator

Before you can install Windows Backup Software, you must download and install the Microsoft iSCSI Initiator 2.x.

To download and install the initiator:

1. Open a Web browser, enter the following in the address bar, and press **Enter**:

   http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-befd1319f825&DisplayLang=en

   Scroll down to the **Files in This Download** section and download the item that ends in x86fre.exe.

2. Select the option to run the file (**Run**, **Open**, or **Run this program from its current location**).

3. If a security warning appears, click **Run**. The installation wizard starts.

4. On the first page of the installation wizard, click **Next**.
5. On the page with installation options, click **Next**. (Initiator Service and Software Initiator are selected by default.)
6. If a message box appears telling you to configure the settings in the Control Panel, click **OK**.
7. If you agree to the terms of the license agreement, select I Agree and then click Next.
8. When the installation completes, click Finish. After your computer restarts, you can install Windows Backup Software.

TECHNICAL NOTE: You do not have to configure the Microsoft iSCSI Initiator. Windows Backup Software will configure it for you automatically.

7.1.4. Installing Windows Backup Software

You must install Windows Backup Software on each computer whose local disks you want to protect. A single license for the Ethernet Disk RAID is located on the back of the unit. Additional licenses can be purchased from http://www.intel.com/design/servers/storage/offers.

To install Windows Backup Software

1. Log on as an administrator and insert the installation CD into a CD-ROM drive.
2. Select **Applications** from the top menu.
3. Select the "**Windows Backup Software**" link to install the software.
4. Start the setup utility for Windows Backup Software.
5. If the Microsoft* iSCSI Initiator 2.0 is already installed, go to the next step. If this component is not currently installed, the prompt in Fig. 7.1.4.B appears.

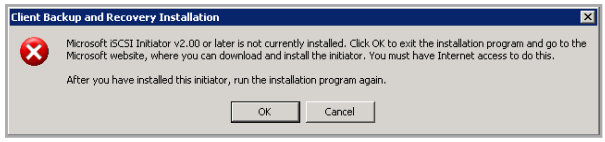

Client Backup and Recovery Installation
Microsoft iSCSI Initiator v2.00 or later is not currently installed. Click OK to exit the installation program and go to the Microsoft website, where you can download and install the initiator. You must have Internet access to do this.
After you have installed this initiator, run the installation program again.
OK
Cancel

Fig. 7.1.4.B

6. Click **OK** to go to the Microsoft website and then click **OK** to cancel the installation of Windows Backup Software.

   On the Microsoft website, click **iSCSI Software Initiator v2.0**, and follow the instructions in section 7.1.3. Installing the Microsoft iSCSI Initiator.

   You must install the Microsoft iSCSI Initiator 2.0 before you can install Windows Backup Software.

   When you have finished installing the iSCSI initiator, re-start the installation of Windows Backup Software.

7. If Microsoft .NET Framework 1.1 is already installed, go to step 9. If this component is not currently installed, the prompt in Fig. 7.1.4.C appears.

   Click **Yes** to install this component. (You cannot install Windows Backup Software without first installing Microsoft .NET Framework 1.1.) When you click **Yes**, the setup utility for Microsoft .NET Framework 1.1 starts.

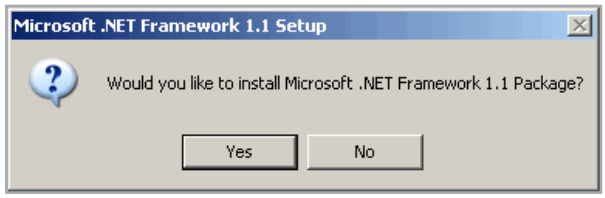


Fig. 7.1.4.C

8. If you agree to the terms of the license agreement, select **I agree** and then click **Install**.

   It might take some time to copy and configure the associated files.

TECHNICAL NOTE: The remaining time might be reported as 0 and it might appear that no progress is occurring. However, configuration is occurring in the background.

9. When a message appears, indicating that the installation of Microsoft .NET Framework 1.1 is complete, click **OK**.

   After you click **OK**, the Intelligent Management Agent is installed automatically (if it is not already installed), and the welcome page for installing Windows Backup Software appears. See Fig. 7.4.1.D.

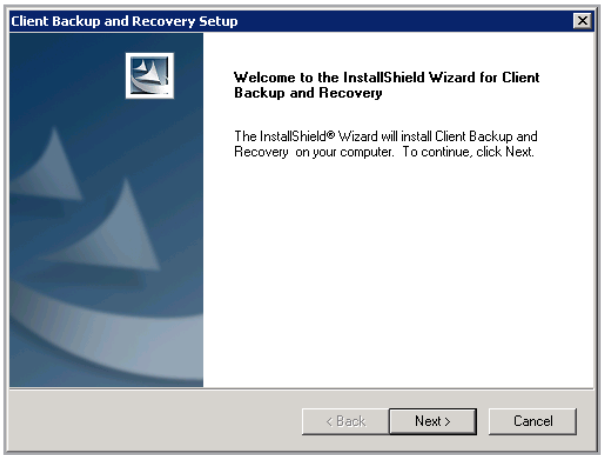

Client Backup and Recovery Setup
Welcome to the InstallShield Wizard for Client Backup and Recovery
The InstallShield® Wizard will install Client Backup and Recovery on your computer. To continue, click Next.
< Back
Next >
Cancel

Fig. 7.1.4.D

10. On the welcome page, click **Next**. The license agreement appears. See Fig. 7.4.1.E.

11. If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and then click **Next**.

12. Click **Next** to install the Windows Backup Software in the displayed location. Alternatively, you can click **Browse**, select or enter a different location, click **OK**, and then click **Next**.

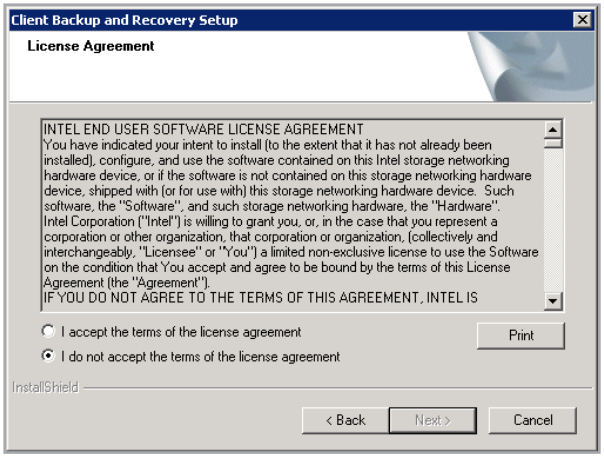

Client Backup and Recovery Setup
License Agreement
INTEL END USER SOFTWARE LICENSE AGREEMENT
You have indicated your intent to install (to the extent that it has not already been installed), configure, and use the software contained on this Intel storage networking hardware device, or if the software is not contained on this storage networking hardware device, shipped with (or for use with) this storage networking hardware device. Such software, the "Software", and such storage networking hardware, the "Hardware". Intel Corporation ("Intel") is willing to grant you, or, in the case that you represent a corporation or other organization, that corporation or organization, (collectively and interchangeably, "Licensee" or "You") a limited non-exclusive license to use the Software on the condition that You accept and agree to be bound by the terms of this License Agreement (the "Agreement").
IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, INTEL IS
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

Fig. 7.1.4.E

IMPORTANT INFO: It is strongly recommended that you install Windows Backup Software on the partition that you boot from (that is, where Windows is installed, typically C:). If you install it on a non-system partition of your system disk, you will not be able to recover that partition using the Client Backup and Recovery application window. In addition, if you plan to remotely boot from a backup on the Ethernet Disk RAID, you must protect the entire disk rather than just the system partition. If you install Windows Backup Software on a different disk than your system disk, you will not be able to remotely boot.

13. To complete the installation and restart your computer, click **Finish**.

    If you do not want to restart your computer at this time, select **No, I will restart my computer later** and then click **Finish**. When the confirmation message appears, click **OK**. You do not have to restart the computer immediately after installation, but you do have to restart it before running Windows Backup Software.

IMPORTANT INFO: If you do not restart your computer and you subsequently reinstall Windows Backup Software, serious problems can occur with your installation. It is strongly recommended that you restart your computer at your earliest convenience.

14. After you restart your computer, click **OK** on the welcome message. The **Add License** dialog box appears. See Fig. 7.1.4.G.

15. Enter the key code for licensing the product and click **OK**. The license key code is located on the back of the Ethernet Disk RAID. If you have an Internet connection, the license is activated automatically. When you click **OK** on the confirmation message, the **Protect a Disk** wizard starts. For information about this wizard, refer to section 7.2. Protecting Your Disks.

If your Internet connection is temporarily down, or if this computer doesn't have an Internet connection, click **OK** on the warning message. The **Protect a Disk** wizard still starts, but after 30 days you will no longer be able to perform backups or recovery until you activate the license. For more information, refer to section 7.1.6. Activating Your License.

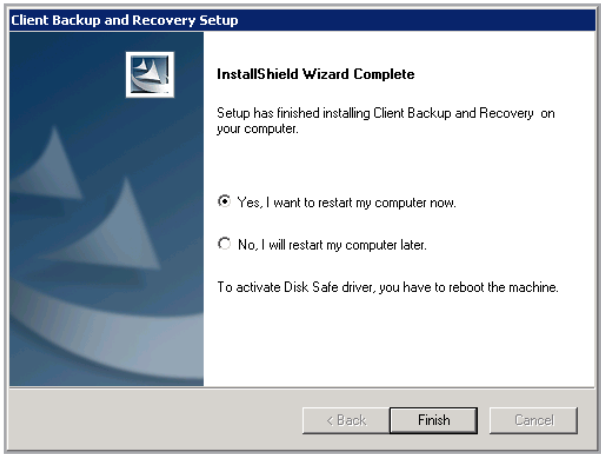

Client Backup and Recovery Setup
InstallShield Wizard Complete
Setup has finished installing Client Backup and Recovery on your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
To activate Disk Safe driver, you have to reboot the machine.
< Back
Finish
Cancel

Fig. 7.1.4.F

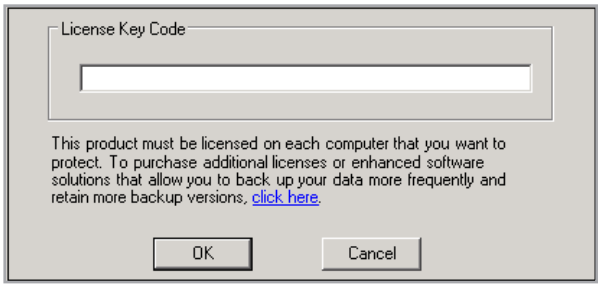

License Key Code
This product must be licensed on each computer that you want to protect. To purchase additional licenses or enhanced software solutions that allow you to back up your data more frequently and retain more backup versions, click here.
OK
Cancel

Fig. 7.1.4.G

IMPORTANT INFO: If you previously used this key code on a different computer, an error message appears, and you must re-activate your license. For more information, refer to section 7.1.6. Activating Your License.

7.1.5. Starting Windows Backup Software

To start Windows Backup Software, do either of the following:

- Click **Start** → **Programs** → **Client Backup and Recovery**
- If the Windows Backup Software Agent is running (as indicated by the presence of the Agent icon ( )) in the system tray), double-click this icon.

If you did not protect a disk after installing Windows Backup Software and restarting your computer, you are prompted to do so the first time you run this application. For information about this wizard, refer to section 7.2. Protecting Your Disks.

If you already protected a disk, the application window in Fig. 7.1.5. appears.

The Status page displays the name of the disk that you protected as well as related information, such as the size of the disk, the name of the Ethernet Disk RAID where the backup resides, the number used to identify the backup disk on the Ethernet Disk RAID (Backup disk ID), the current status, information about any ongoing activity, and the date and time of the last backup and next scheduled backup (if any).

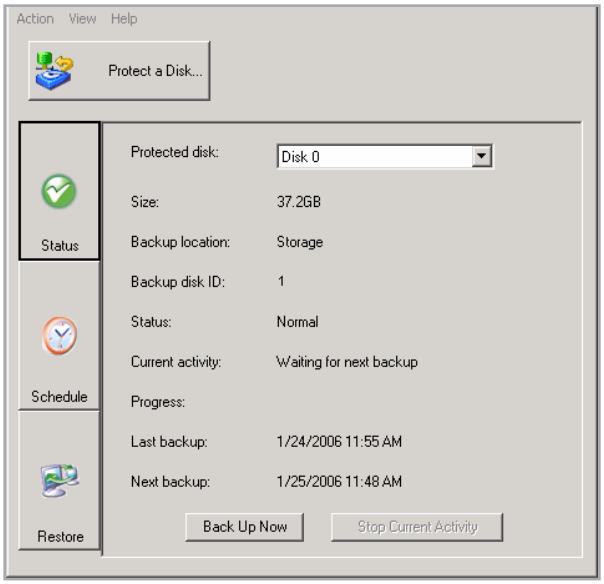


Fig. 7.1.5.

IMPORTANT INFO: If your license is not currently activated, a message appears, advising you of this. You must activate your license within 30 days of installing Windows Backup Software. After that time, you will no longer be able to perform backups or recovery.

7.1.6. Activating Your License

When you install Windows Backup Software and restart your computer, you are prompted to license the product. If your computer has an Internet connection, the license is activated automatically. However, if your Internet connection was temporarily down or if your computer has no Internet connection, your license was not activated. You must activate your license within 30 days of installing Windows Backup Software; otherwise, you will not be able to perform backups or recovery.

If your Internet connection was temporarily down, your license will be activated automatically the next time you run Windows Backup Software with a restored Internet connection.

However, if your computer has no Internet connection, you must perform offline activation (as described in the next section).

IMPORTANT INFO: Activation is tied to your computer's hardware. Once you have activated a particular license, if your computer hardware changes, or if you subsequently install Windows Backup Software on a different computer using the same key code, an error message appears. If this occurs, contact your distributor or reseller to get a new license key through Intel Customer Support.

7.1.7. Activating Your License with an Internet Connection

If your license wasn't activated because your computer has no Internet connection, you must obtain an activation code using another computer that does have both an Internet connection and e-mail.

To activate your license without an Internet connection:

1. From the **Action** menu, click **License** → **Offline Activation**. The Offline Activation dialog box appears.
2. Click **Export License Data**.
3. On the **Save As** dialog box, select one of the following locations and then click **Save**:

- A shared folder accessible to both your computer and a computer that has Internet and e-mail access
- A floppy disk
- A USB disk

4. If you did not save the file to a shared folder, take the floppy disk or USB disk to a computer with Internet and e-mail access.
5. From the computer that has Internet and e-mail access, e-mail the license file to the following address: Activate.Keycode@falconstor.com
6. When you receive an e-mail response, save the returned license file back to the shared folder, floppy disk, or USB disk.
7. If you did not save the file to a shared folder, take the floppy disk or USB disk back to the computer where Client Backup and Recovery is installed.
8. From the Action menu, click **License** → **Offline Activation**.
9. Click **Import Activation Code**.
10. On the **Open** dialog box, browse to the location where the returned license file exists and double-click it.
11. On the confirmation message, click **OK**. The license is now activated and you can continue to back up and recover your disks.
12. To close the dialog box, click **Exit**.

7.1.8. Replacing Your Existing License

1. From the **Action** menu, click **License** → **Add License**. The **Add License** dialog box displays your current license key code.

2. In the **License key code** text box, enter the new key code.

3. Click **OK**.

4. When the confirmation message appears, click **OK**.

If your computer has an Internet connection, the license is activated automatically. If your Internet connection is temporarily down, repeat this procedure when your Internet connection is restored. (You do not have to re-enter the key code.) If your Internet connection is temporarily down, your license will be activated automatically the next time you run Windows Backup Software with a restored Internet connection.

7.2. Protecting Your Disks

After you install Windows Backup Software and restart your computer, the Protect a Disk wizard runs automatically. Using this wizard, you can specify which disk or partition you want to back up, where the backups should be stored, when automatic backups (if any) should occur, and what password you want to use for the recovery CD or booting remotely. If you cancel this wizard, you can start it again at any time using the following procedure.

To protect a disk:

1. Click **Protect a Disk**. The **Protect a Disk** wizard runs.
2. In the **Available disks** list, select the disk or partition that you want to protect. See Fig. 7.2.A.

   Even if your computer has only one hard disk, two items appear in this list. The first item represents the entire hard disk, and the second item represents the partition on that disk. (If there's only one partition on the disk, the partition is the same as the entire disk.)

   If your hard disk is divided into multiple partitions, this list displays one item for the entire hard disk, and one item for each partition. If your computer has multiple hard disks, this list displays an item for each entire disk and an item for each partition on each disk. Each partition is identified by its drive letter.

   If you select an entire disk, all the partitions on that disk are protected as a single entity. This means that you can't later recover only one partition; you have to recover the entire disk. If you select just a partition, you can subsequently recover just that partition.

   In addition, you can recover a data disk or partition using Windows Backup Software, but you can recover a system disk or partition only using the recovery CD or when booting remotely from a backup on the Ethernet Disk RAID. Therefore, if you have separate partitions for your system information and your data, you might want to protect each one separately.

Before you protect a disk, it is recommended that you confirm that sufficient space is available on the Ethernet Disk RAID. At least an additional 20% of the disk size is required for changed data. For example, if the disk that you want to protect is 15 GB, at least 18 GB of space must be available on the Ethernet Disk RAID. The Home page in the Manager (described in section 3.5. Navigating the Manager) displays the amount of available space.

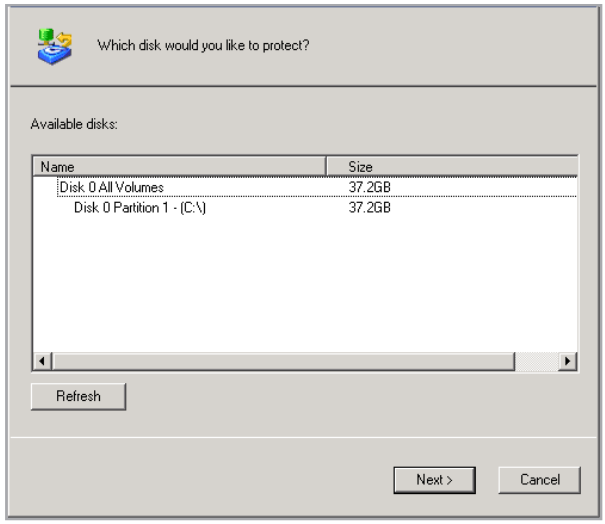


Fig. 7.2.A

TECHNICAL NOTE: Dynamic disks are not supported.

Recommendations:

- If your computer has only one disk with one partition, select the disk.
- If any partition (such as an EISA partition) precedes your system partition, select the entire disk. This ensures that you can remotely boot from and recover the disk.
- If your disk has a system partition and a data partition, select one of the partitions and complete the wizard. Then run the wizard again and protect the other partition. This provides complete protection with maximum flexibility.

  However, if Windows Backup Software was installed on the data partition, protect the entire disk rather than the individual partitions. This ensures that you can remotely boot from that disk.

■ What to do next

In this case	Go to this step
You never previously completed the Protect a Disk wizard	3
You previously completed the Protect a Disk wizard and connected to an Ethernet Disk RAID	4
You previously protected this disk and removed protection (as described in section 7.9.5. Removing Protection)	5

3. When the Add Storage System dialog box appears (Fig. 7.2.B), Client Backup and Recovery automatically scans your subnet for Ethernet Disk RAIDs. Any Ethernet Disk RAIDs that are detected appear in the **Discovered storage systems** list. (It might take a few seconds to complete the scan. You can cancel it at any time by clicking **Cancel** on the scanning message box.)

   From the **Discovered storage systems** list, select the Ethernet Disk RAID where you want to back up the selected disk. The name of the system automatically appears in the **Storage system name** or **IP address** textbox.

   If you plan to remotely boot from a backup on the Ethernet Disk RAID, it is recommeded that you select the IP address of the first port. If the DHCP server option is enabled on your Ethernet Disk RAID, you can remotely boot only from the first port. If this option is disabled and you're using a separate DHCP server, you can remotely boot from either port.

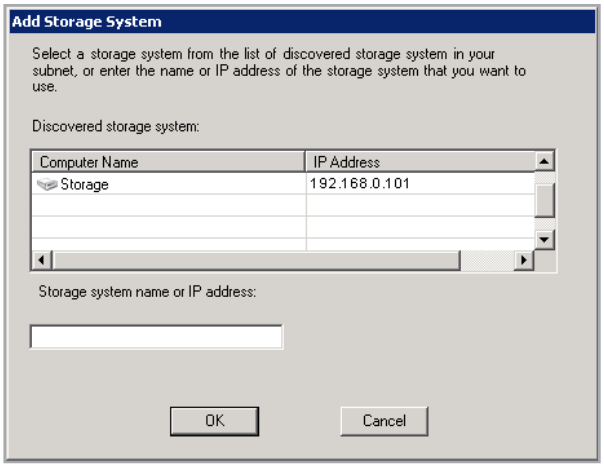

Add Storage System
Select a storage system from the list of discovered storage system in your subnet, or enter the name or IP address of the storage system that you want to use.
Discovered storage system:
Computer Name
IP Address
Storage
192.168.0.101
Storage system name or IP address:
OK
Cancel

Fig. 7.2.B

4. If no Ethernet Disk RAIDs are automatically discovered, or if you want to back up your disk to a different Ethernet Disk RAID, enter the name or IP address of the desired Ethernet Disk RAID in the **Storage system name** or **IP address** text box. Then click **OK**.

5. From the **Backup locations** list, select the Ethernet Disk RAID to use for backups of this disk or partition. (The first backup location in the list is selected by default.) See Fig. 7.2.C.

   If you want to scan the network for new Ethernet Disk RAIDs, or add a new one manually, click **Add** and repeat step 3.

   If you want to remove a Ethernet Disk RAID that's not valid or that you no longer want to use, select the Ethernet Disk RAID from the **Backup locations** list, click **Remove**, and then click **Yes** to confirm the removal. (You can remove an Ethernet Disk RAID only if it is not currently being used to protect another disk.)

   Once you have selected the desired backup location, click **Next** and go to step 6.

TECHNICAL NOTE: If an authentication error occurs, make sure the name or IP address of the Ethernet Disk RAID is correct, and that your computer is connected to the network.

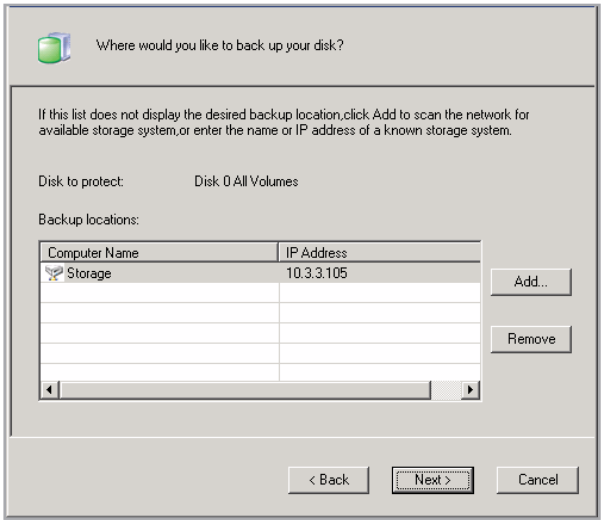

Where would you like to back up your disk?
If this list does not display the desired backup location,click Add to scan the network for available storage system,or enter the name or IP address of a known storage system.
Disk to protect:
Disk 0 All Volumes
Backup locations:
Computer Name
IP Address
Storage
10.3.3.105
Add...
Remove
< Back
Next >
Cancel

Fig. 7.2.C

6. If you previously protected this disk and removed protection, specify whether or not you want to re-use the existing backup or create a new one. See Fig. 7.2.D.

   If you select **Re-use the existing backup**, you must select which backup to re-use from the list. When you select an item from the list, the size also appears to help you identify exactly which backup to use. The word "Preferred" appears for the backup that best matches the disk that you're currently protecting. Once you have selected the desired backup, click **Next** and go to the next step.

   If you select **Create a new backup** and click **Next**, you must select the desired backup location as described in step 4.

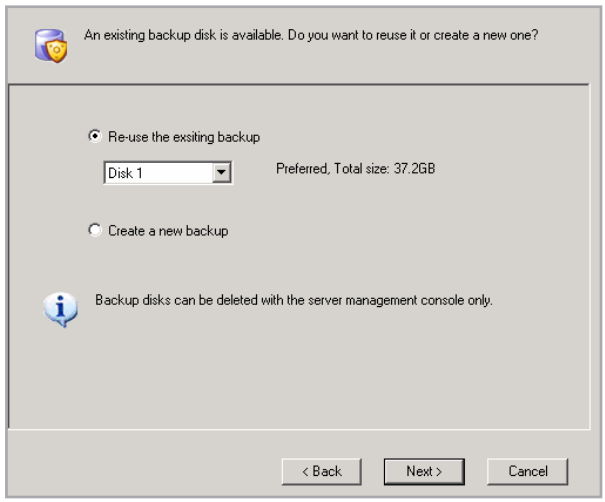

An existing backup disk is available. Do you want to reuse it or create a new one?
Re-use the exsiting backup
Disk 1
Preferred, Total size: 37.2GB
Create a new backup
Backup disks can be deleted with the server management console only.
< Back
Next >
Cancel

Fig. 7.2.D

TECHNICAL NOTE: If the list does not display the expected information, you might need to click **Cancel**, click **Action** → **Repair Connection**, and then try to protect the disk again. Repairing the network connection refreshes the information about the backups that exist on the Ethernet Disk RAID.

CAUTION: If you select any disk other than the preferred one, all the data associated with the selected disk will be overwritten with the data associated with the disk that you're protecting, and you will not be able to recover any previous backups associated with the selected disk.

Specify when you want backups to occur. For example, if you want backups to occur every day, select **Daily** from the **Recurrence** list. If you want backups to occur once a week, select the day of the week from the **Recurrence** list. Then select the time.

If you don't want backups to occur automatically, select **Not Scheduled** from the **Recurrence** list. (The Time list appears dimmed.) Backups will occur only when you start one manually (as described in section 7.3. Manually Backing Up Your Disk).

IMPORTANT INFO: Although Windows Backup Software is specifically designed to perform backups without affecting your other computer activities, you might want to schedule backups for a time when they'll have the least impact on your system, like during lunch or after business hours (if you leave your computer running overnight). If you're protecting multiple disks or partitions, it is recommended that you schedule each backup to occur at a different time.

7. Specify whether or not to back up your disk as soon as you finish the wizard by selecting or clearing the **Back up now** check box, and then click **Next**. See Fig. 6.2-E.

   If you clear this option, the disk will be backed up at the next scheduled time or the next time you perform a manual backup.

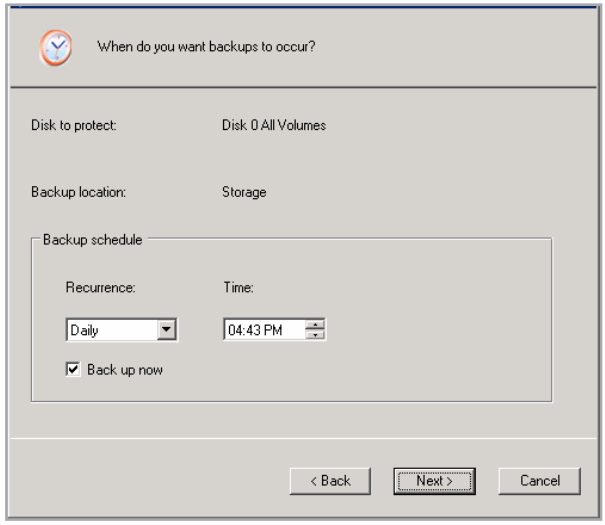


Fig. 7.2.E

IMPORTANT INFO: Only four backups of each protected disk or partition are saved on the Ethernet Disk RAID, so if you back up your disk every day, you'll be able to recover data from only the last four days. If you back up your disk once a week, you'll be able to recover data from four weeks ago, but the most recent backup might be as many as six days old.

IMPORTANT INFO: Be sure to back up your disk or partition before you try to recover it using the recovery CD.

8. If you ever need to recover your disk using the recovery CD or remotely boot from a backup on the Ethernet Disk RAID, you'll be prompted for a password. In the **Recovery password** text box, enter the password that you'd like to use, enter it again in the **Retype your password** text box, and then click **Next**. See Fig. 7.2.F.

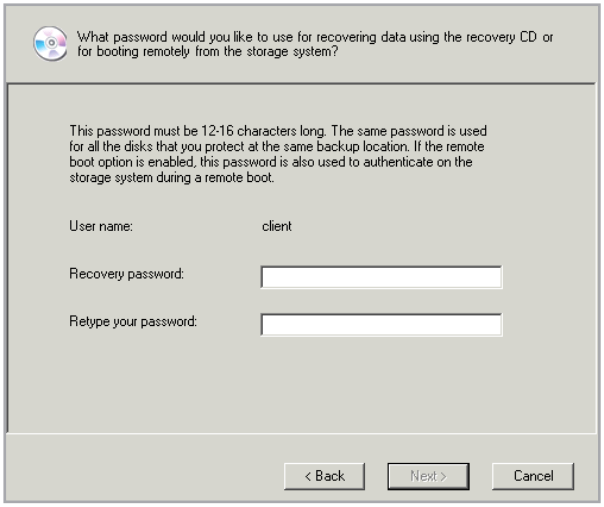

What password would you like to use for recovering data using the recovery CD or for booting remotely from the storage system?
This password must be 12-16 characters long. The same password is used for all the disks that you protect at the same backup location. If the remote boot option is enabled, this password is also used to authenticate on the storage system during a remote boot.
User name:
client
Recovery password:
Retype your password:
< Back
Next >
Cancel

Fig. 7.2.F

TECHNICAL NOTE:

- The recovery password must be 12–16 characters long.
- The same password is used for all disks backed up to the same Ethernet Disk RAID. If you subsequently protect a second disk using the same Ethernet Disk RAID, you will not be prompted to provide this password again. However, if you protect a second disk using a different Ethernet Disk RAID, you will be prompted to provide a password for that Ethernet Disk RAID.
- You can change this password later using Windows Backup Software and using the Ethernet Disk RAID.

9. Review all your selections and click **Finish**. See Fig. 7.2.G.

   If you selected the **Back up now** check box, backup begins as soon as you click **v**, and you can review its progress on the Status page in Client Backup and Recovery. If you want to protect additional disks or partitions, repeat this procedure for each one.

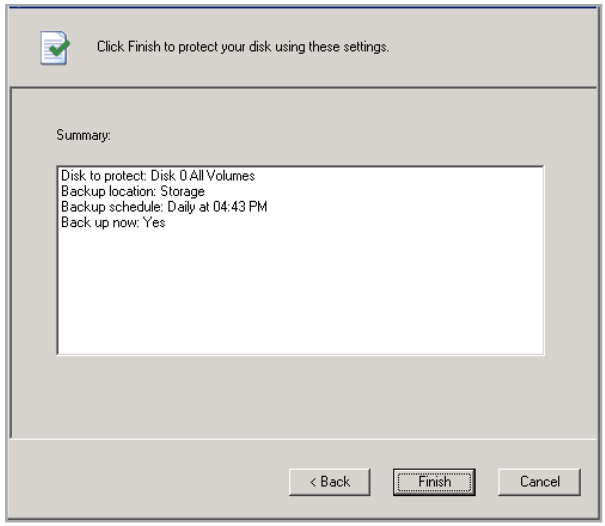


Fig. 7.2.G

IMPORTANT INFO: If you subsequently change the drive letter of a protected disk or partition, you must restart Windows Backup Software to update this application.

7.3. Manually Backing Up Your Disk

Once you protect a disk, it is automatically backed up at regular intervals (unless you chose **Not Scheduled** from the **Recurrence** list when you completed the schedule). You can also back up a disk manually as long as a backup or recovery is not currently occurring. For example, if you're about to install a new application, you might want to back up your disk right before you do that so that if any problems occur, you can recover your disk to the state it was in immediately before you installed the application

To manually back up a disk:

1. Click **Status**.
2. In the **Protected disk** list, select the disk that you want to back up.
3. Click **Back Up Now**. The **Current activity** area displays information about what's happening, the percentage of the backup that has completed, and the speed at which the data is being sent over the network. The **Progress** bar graphically indicates how much of thebackup is complete.

   To stop a backup in progress, click **Stop Current Activity**.

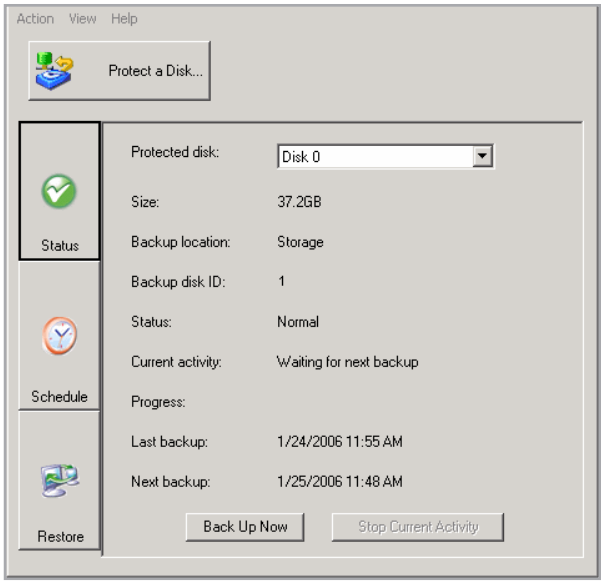


Fig. 7.3.

7.4. Stopping a Backup or Recovery in Progress

Once a backup or recovery starts, you can stop it at any time – for example, if you notice that your system is not responding as quickly as you'd like, and you want to free up processing capabilities for other tasks.

When you stop a backup in progress, that backup won't appear in the list of backups on the Restore page, and any changed data that was not copied to the Ethernet Disk RAID will be copied during the next backup.

When you stop a recovery in progress, the local disk or partition is left in an incomplete state, and you must recover it again later before you can use it.

To stop a backup or recovery in progress:

1. Click **Status**.
2. In the **Protected disk** list, select the disk whose backup or recovery you want to stop.
3. Click **Stop Current Activity**. If you're stopping a backup, the backup stops immediately.

   If you're stopping a recovery, a confirmation message appears. Click **OK** to stop the recovery now, or click **Cancel** to proceed with it.

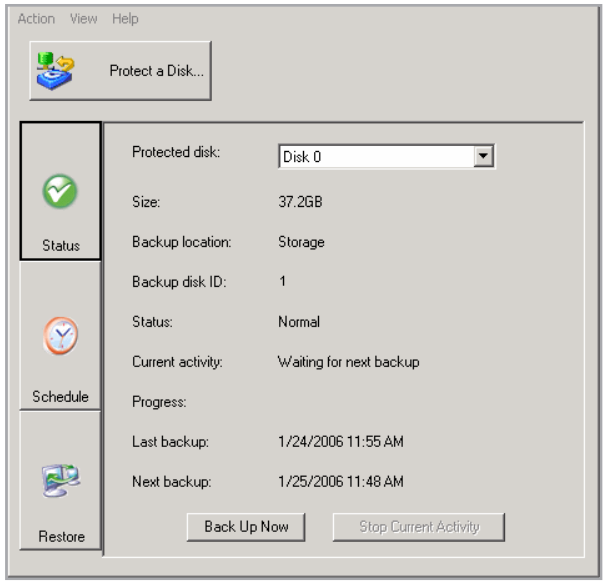


Fig. 7.4.

7.5. Changing the Backup Schedule

When you protect a disk, you specify when you want backups to occur. However, you can change this schedule at any time as long as the Status page indicates that the Status is Normal. If protection is stopped (for example, if you recovered the disk or recovered a different partition on the same disk), you cannot change the disk schedule until you resume protection by clicking **Back Up Now**.

To change the backup schedule:

1. Click **Schedule**.
2. In the **Protected disk** list, select the disk whose backup schedule you want to change.
3. Specify when you want backups to occur.

   For example, if you want backups to occur every day, select **Daily** from the **Recurrence** list. If you want backups to occur once a week, select the day of the week from the **Recurrence** list. Then select the time.

   If you don't want backups to occur automatically, select **Not Scheduled** from the **Recurrence** list. (The **Time** list appears dimmed.) Backups will occur only when you start one manually (as described in section 7.3. Manually Backing Up Your Disk).
4. Click **Apply**.

   The schedule change takes effect immediately, and the date and time of the next scheduled backup appears in the **Next backup** area.

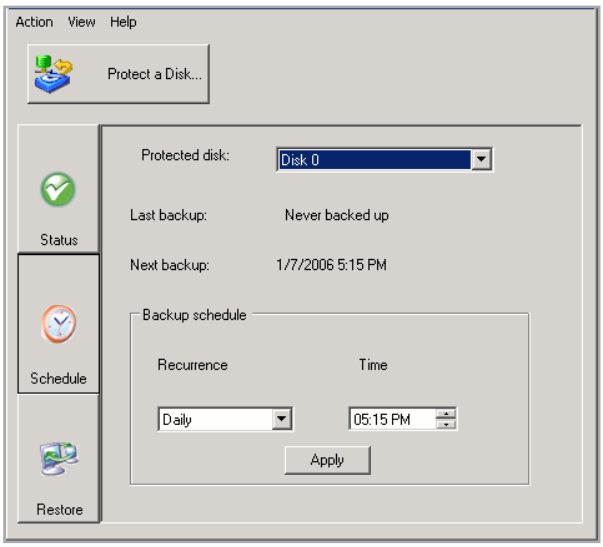


Fig. 7.5.

7.6. Receiving Event Notifications

When you install Windows Backup Software, the Client Backup and Recovery Event Viewer is also installed. This program starts automatically whenever you start your computer, and the Agent icon appears in your system tray.

When the Agent is running, a pop-up message appears whenever a backup-related problem occurs (for example, if a scheduled backup did not occur because the Ethernet Disk RAID was not running).

You can close the Agent at any time. However, if you do this, notifications will no longer appear automatically. If you subsequently want to start the Agent again, you can do so using Windows Backup Software.

To close the Agent:

In the system tray, right-click the Agent icon ( ) and click **Exit Client Backup and Recovery Agent**.

To restart the Agent after you have closed it:

From the **View** menu, click **Agent**. The Agent icon reappears in the system tray.

7.7. Changing the Recovery Password

When you protect a disk, you specify what password to use for recovering the disk using the recovery CD or when you remotely boot from a backup on the Ethernet Disk RAID. You can change this password at any time as long as the Status of the backup is Normal. (This ensures that the change is also made on the Ethernet Disk RAID.)

TECHNICAL NOTE: The same password is used for all disks backed up to the same Ethernet Disk RAID. If you backed up multiple disks to the same location and change the password for one, the password is changed for all of them. However, if you backed up one disk to one Ethernet Disk RAID and a different disk to a different Ethernet Disk RAID, each disk can have a different recovery password.

To change the recovery password:

1. Click **Restore**.
2. In the **Protected disk** list, select a disk whose backup resides on the Ethernet Disk RAID whose recovery password you want to change. See Fig. 7.7.A.

   To double-check your selection, click **Status**. The name of the Ethernet Disk RAID appears in the **Backup location** area. Then click **Restore** to return to the Restore page.

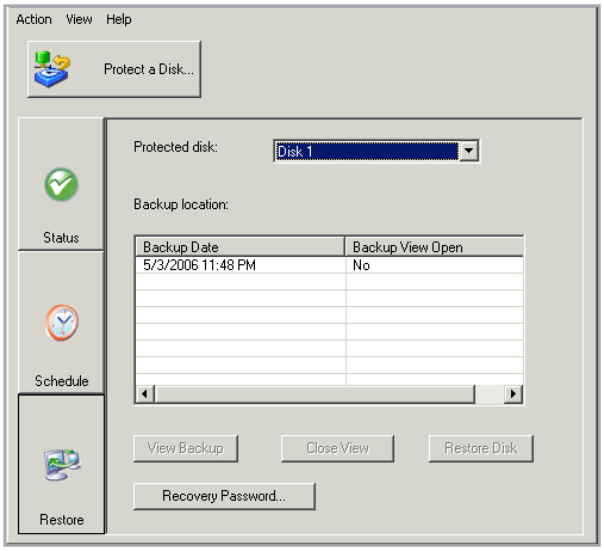


Fig. 7.7.A

3. Click **Recovery Password**. The **Reset Recover Password** dialog box appears. See Fig. 7.7.B.
4. In the **Recovery password** text box, enter the desired password. This password must be 12–16 characters long.
5. In the **Retype your password** text box, enter the password again.
6. Click **OK**.

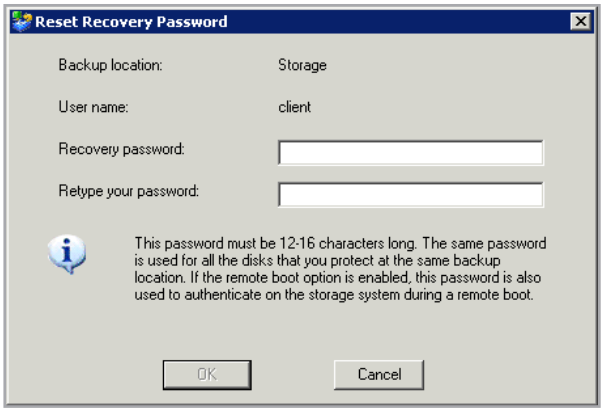

Reset Recovery Password
Backup location:
Storage
User name:
client
Recovery password:
Retype your password:
This password must be 12-16 characters long. The same password is used for all the disks that you protect at the same backup location. If the remote boot option is enabled, this password is also used to authenticate on the storage system during a remote boot.
OK
Cancel

Fig. 7.7.B

7.8. Enabling or Disabling Remote Boot

If you need to recover your system disk or partition, using the recovery CD is recommended (as described in section 7.9.3. Recovering a System Disk Using the Recovery CD). However, if your computer does not support the recovery CD but does support the PXE protocol, you can remotely boot your computer from a backup on the Ethernet Disk RAID and then recover your system disk. (If you're not sure if your computer supports the PXE protocol, try to enable remote boot. If your computer does not support the PXE protocol, an error message will appear during this process.)

You can enable remote boot only if the following criteria have been met:

- Microsoft Windows* was installed on the first partition of the first disk in your computer.
- Windows Backup Software was installed on that system disk.
- You protected your system disk or partition.
- You are accessing the computer directly rather than using Remote Desktop.

When you enable remote boot, your network connection will be temporarily interrupted. It is recommended that you enable remote boot when this will not adversely affect any network applications that you might be running.

If remote boot is successfully enabled, a new backup is created automatically.

Once you have enabled remote boot, if you subsequently want to boot remotely using a different network interface card (NIC), you must first disable remote boot and then enable it again, specifying the other NIC. In addition, after you recover a disk while booting remotely, you must disable and re-enable remote boot.

CAUTION: It is strongly recommended that you determine whether or not your computer supports the recovery CD before a system failure occurs. To do this, perform steps 1 through 3 in section 7.9.3. Recovering a System Disk Using the Recovery CD and use Diagnostic Mode to confirm that at least one network interface card is supported.

If your computer does not support the recovery CD, you must enable remote boot before a system failure occurs. Once your system has failed, you cannot enable remote boot.

If your computer does not support either the recovery CD or the PXE protocol, gather your hardware information (as described in step 4 in section 7.9.3. Recovering a System Disk Using the Recovery CDCD) and send it to your vendor. You might be able to obtain an updated recovery CD or a new driver that will make your computer compatible with your existing recovery CD.

TECHNICAL NOTES:

- If Windows Backup Software was installed on the same disk but a different partition than Windows, the entire system disk must be protected rather than each individual partition. If you protected each partition individually, remove protection for those partitions (as described in section 7.9.5. Removing Protection) and protect the entire disk (as described in section 7.2. Protecting Your Disks).
- You must wait until the initial backup of your system disk or partition has completed before you enable remote boot.

7.8.1. Enabling Remote Boot

To enable remote boot:

1. In the **Protected disk** list on any page, select your system disk or partition. If you protected multiple system disks or partitions, select the first system disk or partition on your computer (typically Disk 0).
2. From the **Action** menu, click **Enable Remote Boot**.

   The **Enable Remote Boot** dialog box appears (see Fig. 7.8.1.A.). This dialog box displays a list of all the NICs on your computer.
3. From the list, select the NIC that you want to use when remotely booting from the Ethernet Disk RAID.

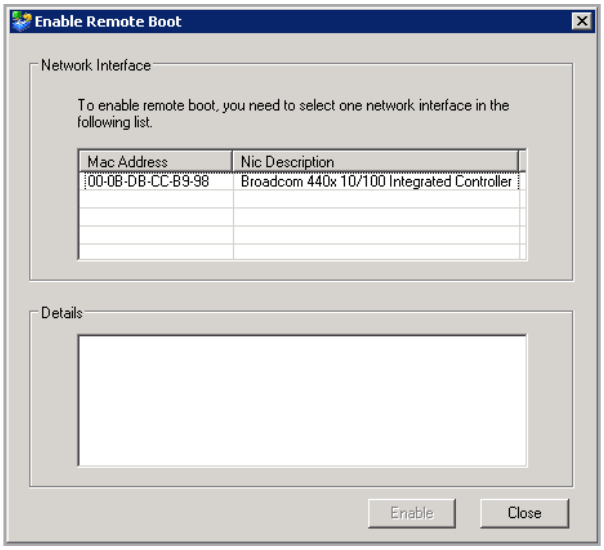


Fig. 7.8.1.A

4. Click **Enable**. A message appears, advising you that your network connection will be temporarily interrupted.
5. Click **Yes** to allow the temporary network interruption. (Your network connection will be restored immediately after this process is complete.)

   On the **Enable Remote Boot** dialog box, the **Details** area shows the progress of the enabling process. If any problems are encountered – for example, if the selected disk or partition was not your system disk – that portion of the process is marked as "Failed." You can click the plus sign next to the process description to expand it and display an error message that explains exactly what happened.

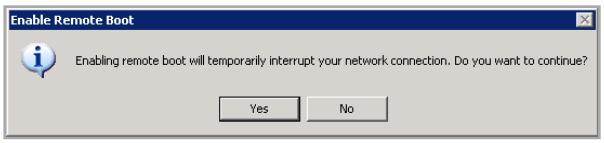

Enable Remote Boot
Enabling remote boot will temporarily interrupt your network connection. Do you want to continue?
Yes
No

Fig. 7.8.1.B

6. When a message appears, advising you that drivers will be installed, click **OK**.

7. When the drivers are installed, one or more messages might appear, advising you that these drivers are not signed. This has no adverse effect on your system. Click **Continue Anyway** or **Yes** on each message to proceed with the installation.

   In addition, the **Found New Hardware Wizard** starts. Select **No, Not this Time** on the initial screen and complete the rest of the wizard, accepting all the default values. If remote boot was successfully enabled (as indicated in the Details area), a new backup is created automatically.

8. Click **Close**.

   If no problems were encountered, you can now remotely boot from the Ethernet Disk RAID (as described in section 7.9.4. Recovering a System Disk While Booting Remotely.)

   If any problems were encountered, take corrective action. For example, if you did not previously protect a system disk or partition, do so now (as described in section 7.2. Protecting Your Disks). Then repeat this procedure for enabling remote boot until all parts of the process complete successfully.

TECHNICAL NOTE: If remote boot was successfully enabled but for some reason the new backup was not created (as indicated in the Details area), you must perform a manual backup (as described in section 7.3. Manually Backing Up Your Disk). You can remotely boot only from backups that were performed after remote boot was enabled.

7.8.2. Disabling Remote Boot

Disabling remote boot restarts your computer automatically. It is recommended that you save and close any open files on your system before you do this.

To disable remote boot:

1. From the **Action** menu, click **Disable Remote Boot**. A progress bar appears, indicating the progress of the process.

2. When the confirmation message appears, click **OK**. Your computer restarts automatically.

7.9. Recovering Data

With Windows Backup Software, there are several ways to recover data from your backups. The best method to use depends on what you want to do and the capabilities of your computer:

Recover selected folders, files, or sections of files if you accidentally permanently deleted a file or folder that you want to recover, or if you just want to retrieve some information from a file that you changed, you can access the backup that contains the desired data and copy it to your local disk.

You can also use this procedure to try out different "what if" scenarios – for example, changing the format of the data in a file – without adversely affecting the data on your local disk.

For more information, refer to section 7.9.1. Recovering Files or Folders.

Recover an entire data disk or partition if you protected a disk or partition that isn't being used to run the operating system, you can recover that disk or partition using Windows Backup Software. You might need to do this if the disk has become corrupted or the data has been extensively damaged. The entire disk or partition will be restored to its exact state at the time of the selected backup.

You can continue to use your computer for other tasks while the data is being recovered, although not any applications or files located on the disk or partition that you're recovering.

For more information, refer to section 7.9.2. Recovering a Data Disk.

Recover an entire system disk or partition if you need to recover your system disk or partition – that is, the disk or partition used to run the operating system – you can do so using the recovery CD. This is particularly useful if the hard disk has failed and has been repaired or replaced, or if you want to duplicate an existing disk to another computer. The entire disk or partition will be recovered to its exact state at the time of the selected backup. However, you won't be able to use your computer until all this process is complete. For more information, refer to section 7.9.3. Recovering a System Disk Using the Recovery CD.

Alternatively, if your computer does not support the recovery CD but does support the PXE protocol, you can boot your computer from a backup on the Ethernet Disk RAID and then recover your system disk. For more information, refer to section 7.9.4. Recovering a System Disk While Booting Remotely.

CAUTION: It is strongly recommended that you determine whether or not your computer supports the recovery CD before a system failure occurs. To do this, perform steps 1 through 3 in section 7.9.3. Recovering a System Disk Using the Recovery CD and use Diagnostic Mode to confirm that at least one network interface card is supported.

If your computer does not support the recovery CD, you must enable remote boot (as described in section 7.8.1. Enabling Remote Boot) before a system failure occurs. Once your system has failed, you cannot enable remote boot.

If your computer does not support either the recovery CD or the PXE protocol, gather your hardware information (as described in step 2 in section 7.9.3. Recovering a System Disk Using the Recovery CD) and send it to your vendor. You might be able to obtain an updated recovery CD or a new driver that will make your computer compatible with your existing recovery CD.

7.9.1. Recovering Files or Folders

To recover selected folders, files, or sections of files from a backup:

1. Click **Restore**.
2. In the **Protected disks** list, select the disk that contains the folders or files that you want to recover.
3. In the **Backups** list, select the backup from the desired date and time. You can select only a backup for which "No" appears in the **Backup View Open** column.
4. Click **View Backup**.
5. When the confirmation message appears, click **OK**.

   After a few moments, a window opens automatically, displaying all the data associated with the selected backup. You can now open the folders and files in the backup view to make sure they contain the information you want, and copy any of the data to your local disk.

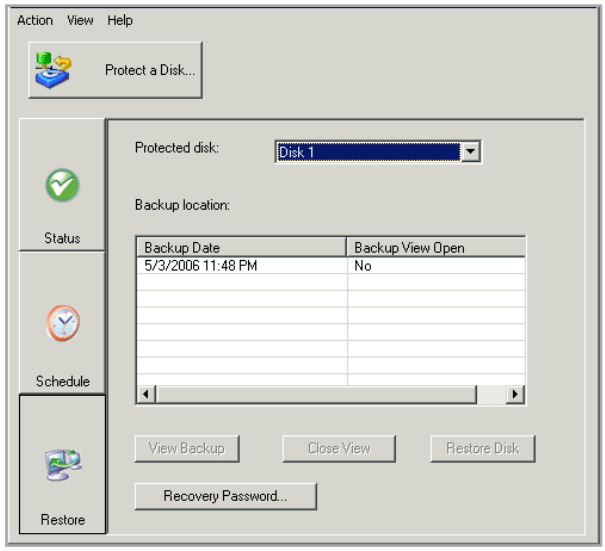


Fig. 7.9.1.

CAUTION: You can open and change the files in the backup view, and even create new folders or files there. However, as soon as you close the view (as described in the next step), all the changes will be lost. The next time you view the backup, it will appear the way it existed at the time the backup was created.

TECHNICAL NOTES:

- If the first drive letter after your local disks is mapped to a shared network folder, you must use Disk Management to change the drive letter assigned to the backup view so that you can access it.

  For example, if your system disk is mapped to C:, your CD-ROM drive is mapped to D:, and a shared network folder is mapped to E:, and you view a backup, you will continue to see the shared network folder when you explore E:, and you will not see a new drive letter for the backup view. (Internally, the backup view is also mapped to E:, since that was the first drive letter after the local disks.) However, when you use Disk Management to change the drive letter for the backup view from E: to F:, you will be able to see both the shared network folder (E:) and the backup view (F:).

  To change the drive letter, right-click My Computer and click Manage. In the left pane, click Disk Management. In the right pane, right-click the backup view, click Change Drive Letter and Paths, click Change, select the desired drive letter from the list box, and then click OK on each dialog box. You can now access the backup view using the specified drive letter.

- If you open a backup view of a disk that contains multiple partitions, a drive letter is assigned to each partition.
- Windows caching can affect the content of the backup view. If the content does not appear to be correct, restart your computer and check again.
- You can view more than one backup simultaneously. Simply repeat steps 3 and 4 for each backup that you want to view.
- If you open a backup view for a partition that cannot be explored (such as an EISA partition), the backup view is closed automatically.
- When a backup view is open, that backup will not be deleted to make room for new backups until it is closed or unless the Ethernet Disk RAID runs critically low on resources. If you view the oldest backup, and the maximum number of backups is reached, new backups cannot occur until the view of the oldest backup is closed (as described in the next step).
- When you close the Windows Backup Software application window, you are prompted to close all open backup views. If you click Yes, both the application window and all open views are closed. If you click No, both the application window and all open views remain open.

6. When you have finished viewing or copying all the desired data, select the backup in the **Backups** list and click **Close View**. The Windows Explorer window closes automatically, and the **Backup View Open** column for the selected backup now displays "No."

7.9.2. Recovering a Data Disk

You can recover a data disk or partition only as long as Windows Backup Software is not installed on that disk or partition, the disk or partition is not currently being backed up, and a more recent backup view is not open.

If you recover a partition and other partitions of that same disk are also protected, protection for those other partitions temporarily stops until the selected partition is recovered.

Once the recovery of any data disk or partition is complete, your computer restarts automatically.

CAUTION: When you recover a data disk or partition, you will lose any data that was written to the disk after the time of the selected backup, as well as any backups that were performed after the backup you're recovering. You might want to copy any newer files that you want to keep to another disk before you recover the disk.

In addition, in rare cases (for example, if your data disk contains applications like antivirus programs that interact with the operating system), if network errors occur or the Ethernet Disk RAID shuts down during recovery, your operating system might become unstable, and you will have to recover it using the recovery CD (or re-install the operating system if you did not protect your system disk).

To recover a data disk or partition:

1. Click **Restore**.
2. In the **Protected disk** list, select the disk or partition that you want to recover.
3. In the **Backups** list, select the backup that you want to recover.
4. Click **Restore Disk**.
5. If you are restoring a partition, and at least one other partition on the same disk is also protected, a message appears, advising you that protection will be stopped for that partition during the recovery process. Click **Yes** to proceed.
6. When the recovery confirmation message appears, click **Yes**.

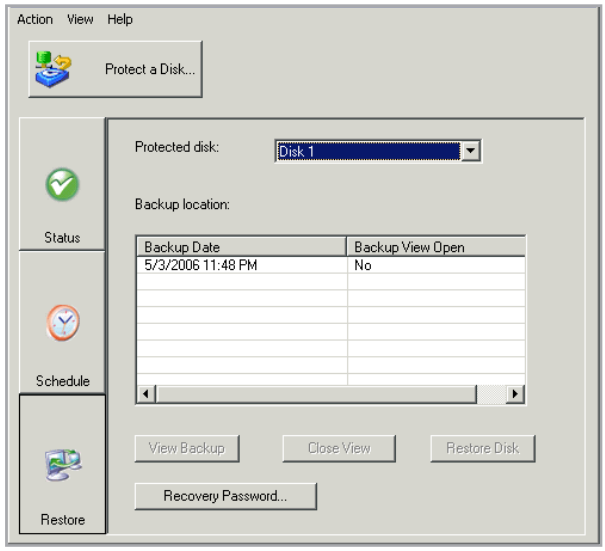


Fig. 7.9.2.

7. If any backup views are open (including backup views of disks other than the one you are recovering), click **Yes** to close them.

   The disk or partition is recovered to exactly its state at the date and time of the selected backup.

   To let you monitor the progress of this activity, the Status page appears automatically. The **Current activity** area displays the percentage of the recovery that has completed,and the speed at which the data is being sent over the network. The **Progress** bar graphically indicates how much of the recovery is complete.

8. When you are prompted to restart the computer, click **OK**.

   You do not have to restart your computer immediately, but you cannot access the recovered disk or partition until you do.

   As soon as you restart the computer, you must start Windows Backup Software and back up the recovered disk or partition manually (as described in section 7.3. Manually Backing Up Your Disk) to resume protection. In addition, if you recovered a partition and any other partitions on the same disk were protected, you must manually back up those partitions as well.

TECHNICAL NOTE: You can cancel this operation at any time by clicking **Stop Current Activity**. However, this will leave the local disk or partition in an incomplete state, and you will have to recover it again before you can use it.

7.9.3. Recovering a System Disk Using the Recovery CD

When you use the recovery CD, you boot your computer from that CD rather than from your local hard disk.

The recovery CD has a menu-style user interface. When responding to the prompts, use the arrow keys to highlight the desired item, use the space bar to select or clear options (an X appears in the brackets when the option is selected), and press Enter to make your selection. You can also tab between fields.

Although the recovery CD is used primarily for recovering a system disk or partition, you can also use it to recover data disks or partitions.

The recovery CD can recover multiple partitions to a disk with existing partitions. It can also create one partition on a new disk. However, if you want to recover multiple partitions to a new disk, you must format and partition the disk before you use the recovery CD to recover the partitions.

TECHNICAL NOTE: The recovery CD does not support USB keyboards or mouse devices.

To recover a system disk or partition using the recovery CD:

1. Using the appropriate procedure for your computer, configure it to boot from the CD-ROM drive.

   For more information, refer to the documentation for your computer.

2. Insert the recovery CD into the CD-ROM drive. A welcome screen appears while the CD initializes.

3. If you have already verified that the recovery CD supports your local hardware, or if you have received a new recovery driver from your vendor, wait 25 seconds for Normal Mode to start automatically and go to step 4.

   If this is the first time you have used the recovery CD, press any key to start Diagnostic Mode. The screen displays a list of all the devices found on your computer and whether or not they are compatible with the recovery CD. You can use the arrow keys to scroll through the list. If at least one supported network interface card (NIC) and one hard disk have been detected, select Normal Mode and go to step 4.

   If no supported NIC is found, you can gather infor

mation about your computer and send it to Technical Support to see if an updated recovery CD or an appropriate driver is available. To do this, select **Save**, insert a formatted floppy disk or USB disk into your computer, and select the appropriate option (**Save to Floppy Disk** or **Save to USB Disk**). Once the file has been saved to the specified location, you can send it to Technical Support. Then select **Finish** and select Yes to restart your computer. At this point, you have 10 seconds to remove the recovery CD from your CD-ROM drive and boot from your local disk once more. Otherwise, your computer will boot from the recovery CD again.

4. When the hardware list appears, take the desired action:

■ Recovery Options

To accomplish this	Do this
Proceed with recovering data	Select **Next**. You can select **Next** only if at least one supported NIC is listed.
Load a new recovery driver	Select **Load Driver**, select the location from which you want to install the driver (**Load From System** for the local hard disk, **Load From Floppy Disk** for a floppy disk, **Load From CD** for a CD, or **Load From USB Disk** for a USB disk), insert the disk (if loading from a floppy disk, CD, or USB disk), and respond to the prompts.
See a complete list of the detected hardware	Select **Diagnostic Mode**. When you are done viewing the list, select **Normal Mode**.

5. Review the network settings for your NIC and select **Next**.

   The recovery CD obtains the IP address to use from your DHCP server. If the displayed settings are not the ones you want to use, or if no IP address is displayed, select the NIC in the list, select **Config**, specify the desired IP address, subnet mask, and default gateway, and select **OK**.

   If multiple NICs are listed, Windows Backup Software will use the last operational one (that is, the last NIC whose Status is Enabled). If you do not want to use the last listed NIC, select **Config**

and then select **Disable** to change the Status to Disabled. Repeat this procedure for each NIC that you do not want to use. Then select **Next**.

6. In the **Computer Name** field, enter the full computer name of this computer.

   If you don't remember the full computer name, access the Manager (as described in section 3.4. Accessing the Manager) and click **Backups** in the navigation bar. In the **Protected disks** group box, the **Computer Name** column lists the computer name of each computer that has backed up disks to the Ethernet Disk RAID.

7. If your computer is a member of a Windows domain, enter the domain name in the **Domain Name** field. (If your computer is not a member of a Windows domain, leave this field blank.)

   Initially, the recovery CD will attempt to connect to the Ethernet Disk RAID using only the computer name. If this fails, the domain name will be appended as well. This ensures that your computer can be properly authenticated.

8. In the **Storage System** field, enter the name or IP address of the Ethernet Disk RAID where the backups reside.

9. In the **Recovery Password** field, enter the recovery password that you specified when you protected the disk or when you last changed the password, and then select Next.

   If you don't remember your password, you can change it on the Ethernet Disk RAID (as described in section 4.4.1. Changing the Recovery Password) and enter the new password here.

   In the left column, select the disk or partition that you want to recover. If you protected only one disk or partition, only one item appears in this list.

   If you protected multiple disks or partitions, you can identify the right item by looking at the **Attr**, **Disk ID**, and **Size** columns. The **Attr** column displays the attributes of each listed item (D for disk, P for parti-

TECHNICAL NOTE: You can use the system name only if your computer is in the same subnet as the Ethernet Disk RAID or if you manually registered the name with a DNS server in your network.

tion, and S for system disk). For example, if you protected both a system partition and a data partition, the system partition will be labeled PS, and the data partition will be labeled simply P. If you protected disks of different sizes, the **Size** column (which displays the number of megabytes) can also help you identify the right item. You can also compare the disk ID with the listed backup disk IDs in the Manager (as described in section 5.6. Managing Backups).

If you protected the same disk more than once (for example, if you remove protection and then protected the disk again without re-using the existing backup), the attributes and size of each backup of that disk will be the same. To determine which item to select, select each one individually and look at the times and dates in the right column. This can help you identify which image is the most recent.

10. In the right column, select the date and time of the backup that you want to recover.

    Whenever you recover data using the recovery CD, an additional backup of the selected backup is created. As a result, if the maximum number of backups has already been performed, the oldest backup is deleted to make room for this backup.

    Backups created by the recovery CD are identified in this list by the word <Recovery>. To update the information on this screen, select **Refresh**. This is helpful if you're recovering data from one computer to another and a new disk was protected or a backup occurred after this screen was displayed.

11. Specify whether or not to delete all backups that occurred after the selected date by selecting or clearing **Delete all later backups**.

12. Specify whether or not to scan for differences between the backup and your local disk by selecting or clearing **Enable microscan**, and then select **Next**.

CAUTION: Selecting a backup with a specific date/time stamp is strongly recommended.

In most cases, selecting **Latest Backup** is the same as selecting the backup in the list with the most recent date/time stamp. However, if the most recent backup is marked <Protect>, the Latest Backup will be in an incomplete state. In that case, be sure to select one of the other listed backup dates rather than Latest Backup.

In addition, if nothing appears in this column besides Latest Backup, do not recover this disk or partition. In this situation, Latest Backup represents only the empty storage space allocated for the backup and contains no data to recover.

CAUTION: This action is not reversible. If you select this option, you will not be able to subsequently recover from another later backup.

In addition, you can select this option only if you selected an older backup from the list; you cannot select this option if you selected <**Latest Backup**>.

13. If you're simply overwriting corrupted data on the same disk that you protected previously, select this option. Only the data that differs between the backup and the local disk will be copied to the local disk. This can minimize the impact to the network, although the scanning process takes some additional time.

    If you're recovering the backup to a brand new disk, clear this option. All the data from the backup will be copied to the new disk without any scanning (there will be nothing to scan on the new disk).

14. Select the local disk where you want to recover the data, and select **Next**.

15. If you selected a disk in step 10, go to step 18. If you selected a partition in step 10, select **Restore** to a partition to recover to an existing partition on the selected disk, or select **Clear all partitions and create new** to delete all the existing data on the selected disk and recover only the selected partition.

16. If you selected **Restore** to a partition in step 15, select the partition where you want to recover the data, and then select **Next**. (Otherwise, go to step 18.) For system partitions, the Active column displays Yes.

17. If the selected partition is not the original partition, select **Yes** to use the selected partition. Otherwise, select **No** and select a different partition.

18. Select **Yes** to confirm the recovery.

    The status screen displays the progress of the recovery. You can cancel it at any time by selecting **Cancel**. However, this leaves the disk or partition in an incomplete state (some of the data will have been recovered, but not all of it).

TECHNICAL NOTE: If you replaced the original hard disk, the new disk must be at least as large as the original disk. In addition, if you are recovering a system disk, the system to which you are recovering the data must be identical to the original system. For example, if the original system had a particular type of network adapter, the system to which you are recovering the data must have the exact same type of network adapter. Otherwise, the recovered files will not operate properly.

CAUTION: This overwrites any existing data on the selected disk. Although you can subsequently recover different data, you cannot recover the original data.

19. When the completion screen appears, review the results and do one of the following:

■ Recovery Options

To accomplish this	Do this
Recover another disk or partition	Select Recover Another Disk. If you want to recover a different backup of the same computer from the same Ethernet Disk RAID, select Yes to retain the current configuration settings and return to step 10. If you want to recover a different computer's backup, or if you want to recover a backup from a different Ethernet Disk RAID, select No to modify the current configuration settings and return to step 6.
Restart the computer	Select Restart Computer. When the informational message appears, select OK. When prompted to confirm that you want to restart the computer, select Yes. You have 10 seconds to remove the recovery CD from the CD-ROM drive.

20. When the computer restarts, use the appropriate procedure for your system to configure the computer to boot from the local hard disk once more.

    If you changed the recovery password on the Ethernet Disk RAID, reset it in the Microsoft iSCSI Initiator* (as described in section 8.4. Resetting the Recovery Password in the Microsoft iSCSI Initiator).

    Start Windows Backup Software and remove protection from the recovered disk or partition (as described in section 7.9.5. Removing Protection).

    Protect the recovered disk once again (as described in section 7.2. Protecting Your Disks), re-using the original backup.

7.9.4. Recovering a System Disk Using While Booting Remotely

If your computer meets the necessary prerequisites, you can remotely boot it from a backup on your Ethernet Disk RAID and recover your system disk or partition. You can recover only your most recent backup.

Prerequistites

Before you recover a disk while booting remotely, the following criteria must be met:

- The computer that you're remotely booting must be in the same subnet as the Ethernet Disk RAID.

  Remote boot must be enabled for that computer (as described in section 7.8.1. Enabling Remote Boot).

- At least one backup must have been performed after remote boot was enabled.

  The network must have a DHCP server, or your Ethernet Disk RAID must be configured to act as a DHCP server (as described in section 5.7.5. Network).

- If you plan to remotely boot your computer from a different computer's backup, you must enter the MAC address of your computer's network interface card (NIC) on the Ethernet Disk RAID. For more information, refer to section 4.4.2. Configuring Remote Boot.

- If you want to remotely boot from any backup other than the most recent one, you must select the desired backup on the Ethernet Disk RAID. For more information, refer to section 4.4.2. Configuring Remote Boot.

IMPORTANT INFO: If you replaced the original hard disk, the new disk must be at least as large as the original disk. In addition, the system to which you are recovering the data must be identical to the original system. For example, if the original system had a particular type of network adapter, the system to which you are recovering the data must have the exact same type of network adapter. Otherwise, the recovered files will not operate properly.

Recovering the Disk

1. Start your computer.
2. Use the appropriate procedure for your system to configure it to boot from the NIC.

   For example, you might press F12 when the boot menu appears. For more information, refer to the documentation for your computer.

   When the computer restarts, allow it to boot from the NIC. (You might be prompted to press F1 to continue.)
3. When prompted, press F8. You have a limited amount of time to do this.
4. Using the arrow keys, select **Remote Boot** (Windows) and then press **Enter**.
5. When prompted, enter the password that you specified when you protected the system disk or when you last changed the password for that disk.

   If you don't remember your password, you can change it on the Ethernet Disk RAID (as described in section 4.4.1. Changing Recovery Password) and enter the new password.
6. If any error messages appear, click **OK**.
7. Log in as you normally would. The message Network Boot Mode appears on the screen to confirm that you are working from the Ethernet Disk RAID.

CAUTION: You can open and change files while remotely booting, and even create new files or folders. However, only the data that existed at the time and date of the selected backup will be recovered. If you want to save any new data, you must copy the files or folders to a different location, such as a network server.

8. Start Windows Backup Software.
9. When a warning message appears, advising you that the computer name has changed, click **OK**.

CAUTION: While booting remotely, do not try to use Windows Backup Software for any operation other than recovering the system disk.

10. Click **Restore**.

    The **Protected disk** list displays the disk or partition that you are currently booting from. See Fig. 7.9.3.1-A.

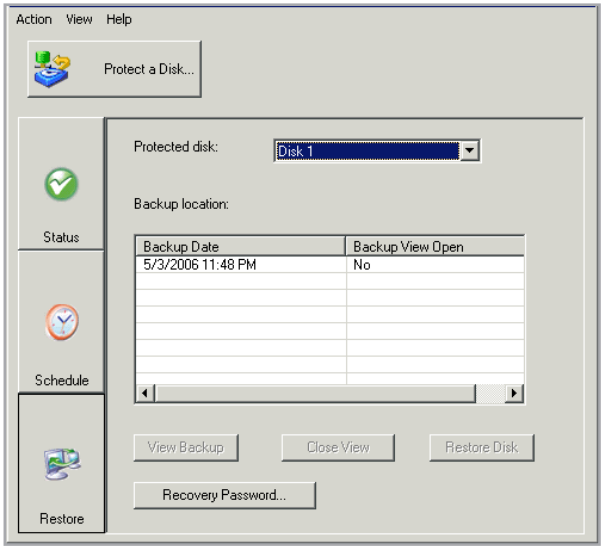


Fig. 7.9.4.A

11. In the **Backups** list, select the most recent backup. You cannot recover any backup except the most recent one.

TECHNICAL NOTE: If no backups appear in this list, the backup that you booted from is not using the same recovery password as the Ethernet Disk RAID. This can occur if you changed the recovery password on the Ethernet Disk RAID before booting remotely, or if you changed it between backups in Windows Backup Software and booted from an earlier backup. To resolve this issue, you must reset the password in the Microsoft iSCSI Initiator* (as described in section 8.4. Resetting the Recovery Password in the Microsoft iSCSI Initiator). Then restart Windows Backup Software.

12. Click **Restore Disk**. The Restore dialog box appears. See Fig. 6.9.3.1-B.

13. Specify whether you are recovering to the original disk or a new disk. If you are recovering to a new disk, select the desired disk from the list. Then click **Restore**.

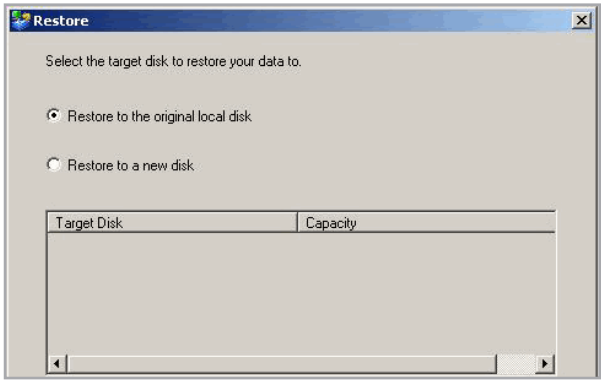

Restore
Select the target disk to restore your data to.
Restore to the original local disk
Restore to a new disk
Target Disk
Capacity

Fig. 7.9.4.B

14. When the confirmation message appears, click **Yes**. The backup is recovered to your local disk, and the progress bar displays the progress of this process. You can cancel the recovery at any time by clicking **Stop** on the progress dialog box.

15. After the recovery is complete, click **OK** to restart your computer.

16. Use the appropriate procedure for your computer to configure it to boot from the local disk once more.

17. If you changed the recovery password, reset it in the Microsoft iSCSI Initiator* after your computer restarts (as described in section 8.4. Resetting the Recovery Password in the Microsoft iSCSI Initiator).

18. Start Windows Backup Software and remove protection from all your disks and partitions (as described in section 7.9.5. Removing Protection). Then protect them again (as described in section 7.2. Protecting Your Disks), reusing the existing backups.

    If you need to recover other data disks or partitions, you can do so (as described in section 7.9.2. Recovering a Data Disk). However, be sure to do this after you have removed protection and then reprotected the disks.

19. Disable remote boot (as described in section 6.8.2. Disabling Remote Boot) and enable it again (as described in section 7.8.1. Enabling Remote Boot).

IMPORTANT INFO: Do not shut down your computer, disconnect from the network, or perform any other tasks until this process is complete.

7.9.5. Removing Protection

If you no longer want to back up a particular disk or partition, you can remove protection as long as a recovery is not currently in progress for that disk or partition. (If a recovery is in progress, you must cancel it or wait until it completes before you can remove protection.)

When you remove protection for a disk for which remote boot is enabled, remote boot will be disabled and your computer will restart.

When you remove protection, you will no longer be able to back up the selected disk or partition either automatically or manually, and you cannot recover data using Client Backup and Recovery (as described in section 7.9.1. Recovering Files or Folders and section 7.9.2. Recovering a Data Disk). However, the backups that currently exist on the Ethernet Disk RAID are retained, and you can recover them using the recovery CD (as described in section 7.9.3. Recovering a System Disk Using the Recovery CD).

If you subsequently want to protect the same disk or partition again, you can re-use the existing backups. You can also delete the existing backups on the Ethernet Disk RAID to free up space for backups of other disks or partitions, either for this computer or other computers. For more information, refer to section 5.6.3. Deleting a Backup.

TECHNICAL NOTE: If you plan to delete a protected partition, be sure to remove protection before you delete that partition. Otherwise, you might not be able to protect other partitions on that disk.

To remove protection:

1. In the **Protected disk** list on any page, select the disk for which you want to remove protection.
2. From the **Action** menu, click **Remove Protection**.
3. When the confirmation message appears, click **Yes**.

The disk disappears from the **Protected disk** list. If another disk is protected, that disk appears in the **Protected disk** list, and information about that disk now appears in the application window. If no other disk is protected, click **OK** on the informational message; the **Protected disk** list and application window are blank.

4. If remote boot was enabled, it is disabled. When prompted, click **OK** to restart your computer.

8. Troubleshooting

This section provides general information about common problems that you might have with your Ethernet Disk RAID and Windows Backup Software and steps you can take to resolve them.

8.1. Troubleshooting the Ethernet Disk RAID

Problem	Solution
I can't access the Manager.	This can occur if you attached the network cable after powering on the Ethernet Disk RAID. Shut down the Ethernet Disk RAID, make sure the network cable is attached, and power it on again. If you're using the Console, make sure the computer where the Console is installed is in the same subnet as the Ethernet Disk RAID. If you're using a Web browser, make sure the name or IP address of the Ethernet Disk RAID is correct. You can use the system name only if your computer is in the same subnet as the Ethernet Disk RAID, if you added the Ethernet Disk RAID's IP address and name to your local hosts file, or if you manually registered the name with a DNS server in your network. In addition, if you configured the Ethernet Disk RAID to use a specific IP address, you might need to specify the IP address of the gateway in your network before you can successfully access the Manager using a Web browser. First access the Manager using the Console (as described in section 3.5. Logging In to the Manager) and then specify the gateway address (as described in section 5.7.5. Network .) and try to access it using a Web browser.
I forgot the password for logging in to the Manager.	You can reset the Ethernet Disk RAID to use its original administrator user name (admin) and password (storage) by pressing the small, recessed reset button on the back of the unit. **NOTE:** This also resets the Ethernet Disk RAID to its original network settings. If you previously configured the Ethernet Disk RAID to use a specific IP address, it will now obtain its IP address from the DHCP server (if any). If you don't have a DHCP server on the network, it will use its default IP address (192.168.0.101). For information about changing these settings, refer to section 5.7.5. Network . In addition, pressing this button restarts the Ethernet Disk RAID, which might adversely affect user connections to shared folders. Be sure to do this only when users are not connected to shared folders or performing recovery.

Problem	Solution
The users can't access the shared folders.	❖ Make sure the Ethernet Disk RAID is powered on, connected to the network, and operating properly. ❖ Make sure the user configuration is correct. For Windows or Mac OS X users, try changing the password (as described in "Modifying Users" on page 42) and accessing the shared folder again. For Linux users, make sure the computer name or IP address is correct. If it's not, recreate the user by removing the existing user (as described in section 5.4.3. Removing Users) and adding it again (as described in section 4.1.1. Adding Users). ❖ Make sure the users are using the proper procedure for accessing the shared folders (as described in section 6.1. Accessing Shared Folders), including the correct name or IP address of the Ethernet Disk RAID. (Windows* and Mac OS X users can use the Ethernet Disk RAID name only if their computer is in the same subnet as the Ethernet Disk RAID, if they added the Ethernet Disk RAID's IP address and name to their local hosts file, or if the Ethernet Disk RAID name was manually registered with a DNS server in your network. Linux users must use the IP address.) Windows users can't access shared folders using the Console unless their computers are on the same subnet as the Ethernet Disk RAID. If using the Console does not work, try accessing the shared folders using My Computer or Windows Explorer (as described in section 6.1.1.1. Using My Computer or Windows Explorer). ❖ Make sure the user's computer is connected to the network and can otherwise access the Ethernet Disk RAID. To check the network connection in a Windows environment, click Start --> Run and type cmd. At the command prompt, type the following: ping IP_address where IP_address is the IP address of the Ethernet Disk RAID. If you do not see Reply from..., the problem is with your network.
The users can't create files in the shared folders.	Check the access rights for the user (as described in section 5.5.2. Changing User Access to Shared Folders). The user must have read/write rights to be able to create files in the shared folder.
The Ethernet Disk RAID is not distributing IP addresses.	Make sure that Enable DHCP server is selected on the Network page (as described in section 5.7.5. Network) and that the starting and ending IP addresses are valid. The first three digit groups of both the starting IP address and ending IP address must be the same. If the network configuration is correct and it still doesn't work, the DHCP service might not be working properly. Restart the Ethernet Disk RAID.

Problem	Solution
The users cannot access the Ethernet Disk RAID using FTP.	Make sure that Enable FTP server is selected on the Network page (as described in section 5.7.5. Network) and that the users are using the correct address for accessing the Ethernet Disk RAID (as described in section 5.7.6. Reconfiguring the Disks). If the network configuration is correct and the users are using the proper address and it still doesn't work, the FTP service might not be working properly. Restart the Ethernet Disk RAID.
A package size error appears when I upgrade the firmware	If you downloaded the firmware from a website or copied it from a CD, compare the original size of the package file with the size of the package file that you're using. If they differ, download or copy the file again to ensure that it is not corrupted. If the problem persists, restart the Ethernet Disk RAID before upgrading the firmware. This ensures that any temporary files on the Ethernet Disk RAID are deleted before the firmware is upgraded.

8.2. Troubleshooting Windows Backup Software

Problem	Solution
The disk that I want to protect isn't listed.	Windows Backup Software does not support dynamic disks. These types of disks are automatically filtered from the list of disks that you can protect.
Errors occur when I try to protect a disk.	❖ When adding a storage system to the list of backup locations, make sure that you're using the correct name or IP address of the storage system. ❖ If the storage system is already listed, select it in the list of backup locations and then click Remove. Then click Add to add it again. This resets the settings in the Microsoft iSCSI Initiator* which might cause authentication problems. ❖ Make sure the storage system is powered on. ❖ Make sure the computer is connected to the network and can otherwise access the storage system. To check the network connection, click Start --> Run and type cmd. At the command prompt, type the following: ping IP_address where IP_address is the IP address of the storage system. If you do not see Reply from..., the problem is with your network. ❖ Make sure that sufficient space is available on the storage system. At least an additional 20% of the disk size is required for changed data. For example, if the disk that you want to protect is 15 GB, at least 18 GB of space must be available on the storage system. The Home page in the Manager displays the amount of available space. **NOTE:** If errors occur when you're protecting a disk for the first time, invalid backups might be created on the storage system. To ensure that you don't use up disk space unnecessarily, be sure to delete any extraneous backups on the storage system (see section 5.6.3, Deleting a Backup). Compare the Backup disk ID on the Status page in Windows Backup Software with the Backup Disk ID on the Backups page in the Manager to determine which backup is actually being used.

Problem	Solution
The Status page indicates that the backup is offline.	❖ Make sure the storage system is powered on. ❖ Check the network connection to the storage system. To do this, click Start --> Run and type cmd. At the command prompt, type the following: ping IP_address where IP_address is the IP address of the storage system. If you do not see Reply from..., the problem is with your network. ❖ Click Action --> Repair Connection to refresh the network connection. ❖ Make sure that the backup has not been deleted on the storage system by checking the Backups page (see section 5.6, Managing Backups). If it has been deleted, remove protection (see section 7.9.5, Removing Protection) and protect the disk again (see section 7.2, Protecting Your Disks). ❖ If you changed the name of your computer, the storage system will not recognize it any longer. Remove protection for all your disks or partitions (see section 7.9.5, Removing Protection), delete the old computer name from the storage system (see section 5.6.4, Deleting a Client), and then protect your disks again (see section 7.2, Protecting Your Disks).
A backup did not occur at its regularly scheduled time.	❖ Check the schedule (see section 7.5, Changing the Backup Schedule) to confirm that it is correctly configured. ❖ Make sure the computer is powered on during the scheduled backup time. ❖ Make sure the storage system is powered on during the scheduled backup time. ❖ On the Status page, make sure that the Status is Normal. If protection is stopped (for example, if you recovered the disk or recovered a different partition on the same disk), backups will not occur until you resume protection by clicking Back Up Now. If the Status is Offline, review the troubleshooting procedures in the preceding section. ❖ If you changed the name of your computer, the storage system will not recognize it any longer. Remove protection for all your disks or partitions (see section 7.9.5, Removing Protection), delete the old computer name from the storage system (see section 5.6.4, Deleting a Client), and then protect your disks again (see section 7.2, Protecting Your Disks). ❖ If the IP address of the storage system changed (for example, if the storage system obtains its IP address from a DHCP server and acquired a new one after you added the storage system to the list of backup locations), you must start Windows Backup Software so that it can retrieve the new IP address. You must do this each time the IP address on the storage system changes.
I can't change my backup schedule.	On the Status page, make sure that the Status is Normal. If protection is stopped (for example, if you recovered the disk or recovered a different partition on the same disk), you cannot change the schedule until you resume protection by clicking Back Up Now.

Problem	Solution
I forgot my recovery password.	Reset the password using the storage system (see section 5.6, Managing Backups). Once you reset it on the storage system, you can use the new password with the recovery CD or for booting remotely from the storage system.

8.3. Creating a Diagnostic File

In some cases, you might need assistance from Customer Support to solve problems that you might have with Windows Backup Software. When you contact the Customer Support team, they might ask you to create a diagnostic file to help them better understand your environment and configuration settings.

You can create a diagnostic file using either the Windows Backup Software application or, in the event of a system failure, using the recovery CD. To create a diagnostic file using the recovery CD, the computer must have a floppy disk drive or a directly connected USB disk.

IMPORTANT INFO: This diagnostic file does not include the log files associated with the Intelligent Management Agent (IMA). You might be asked to send those files (iscmlib.log and iscmservice.log) separately.

8.3.1. Using Windows Backup Software

To create a diagnostic file using Windows Backup Software:

1. Run Windows Backup Software.
2. From the Action menu, click Create Diagnostic File.
3. Click Save to save the file using the default file name, or type the desired file name in the File name text box and then click Save. If desired, you can save the file in a different location. Once the file has been created, you can send it to Customer Support.

8.3.2. Using the Recovery CD

To create a diagnostic file using the recovery CD:

1. Insert the recovery CD into the computer's CD-ROM drive.
2. After the CD has initialized, press Alt+F2.
3. At the command line, enter the following command and then press Enter: xray
4. When prompted, enter your e-mail address and press Enter. This ensures that your e-mail address is saved as part of the diagnostic file in case Customer Support needs to contact you.
5. When prompted, insert a formatted floppy disk into the computer's floppy disk drive or attach a USB disk and press Enter.
6. When the list of destination options appears, enter the appropriate number and press Enter. When a message appears, indicating that the file has been created, you can send it to Customer Support.
7. To return to the recovery CD menu, press Alt+F1.

8.4. Resetting the Recovery Password in the Microsoft iSCSI Initiator

The recovery password used by the recovery CD and for booting remotely is actually the Microsoft iSCSI Initiator* CHAP secret. When you protect a disk or change the recovery password using Windows Backup Software, the Microsoft iSCSI Initiator* is configured automatically.

If you forget this password, you can reset it on the storage system. However, if you do this when your system is down (that is, while you're booting from the recovery CD or booting remotely), the recovery password in your Microsoft iSCSI Initiator* will not match the recovery password on the storage system. As a result, when you recover your system disk using the recovery CD and then boot from the local disk, you will not be able to connect to the storage system. Likewise, when you boot remotely, you will not be able to recover your disks at all.

This problem can also occur if you change the recovery password between backups using Windows Backup Software and then remotely boot from one of the earlier backups. In this case as well, the recovery password in the Microsoft iSCSI Initiator* will not match the recov ery password on the storage system.

To address this issue, you must reconfigure the Microsoft iSCSI Initiator* to use the password that you specified on the storage system. If you're using the recovery CD, you must do this after you recover your system disk. If you're booting remotely, you must do this while in Network Boot Mode (before you recover your system disk) and again after you recover your disk and boot locally.

To reset the recovery password in the Microsoft iSCSI Initiator*:

1. Click Start --> Programs --> Microsoft iSCSI Initiator --> Microsoft iSCSI Initiator.
2. Click the Targets tab.
3. If more than one target appears in the Targets list, select the one that contains the name of the storage system. The Status should be Disconnected.
4. Click Log On.
5. Click Advanced.
6. Select the CHAP logon information check box.
7. In the User name text box, type your computer name in all capital letters.
8. In the Target secret text box, type the recovery password that you specified on the storage system.
9. Click OK on the Advanced Settings and Log On to Target dialog boxes. The Status of the target should now be Connected.
10. Click OK on the iSCSI Initiator Properties dialog box.

9. Technical Specifications

9.1. Hardware Specification

Component	Specification
Processor	400-MHz Intel® IOP80219
Memory	256 MB 32-bit DDR SDRAM
Flash	32-MB NOR Flash
Hard Drive	Supports up to four 3.5-in SATA-I hard drives from 80 GB to 500 GB **NOTE:** The total amount of storage space cannot exceed 2 terabytes (at the date of publication).
Network	Two Intel® gigabit LAN port interface
USB	Two USB 2.0 connectors
EMI Safety	CE/FCC Class B
System Power	200-W power supply
Operating Temperature	10° C to 35° C (50° F to 95° F)

TECHNICAL NOTE: If the temperature of the processor reaches or exceeds 85° C (185° F) or if the temperature of any of the backplane temperature sensors reaches or exceeds 55° C (131° F), the Ethernet Disk RAID shuts down automatically. If the temperature of any of the backplane temperature sensors reaches or exceeds 42° C (107.6° F), the fan will run at full speed. If, subsequently, the temperature of any of the backplane temperature sensors reaches or falls below 37° C (98.6° F), the fan will return to normal speed.

9.2. Software Specification

Component	Specification
Operating System	Linux Kernel 2.6.10
Network Service	DHCP client/server (default IP address for Port 1 is 192.168.0.101)
Supported Web Browsers	❖ Microsoft Internet Explorer 6.0* ❖ Firefox* 1.06 or newer
RAID	❖ Standard RAID 0 ❖ RAID 1 ❖ RAID 5 ❖ RAID 5 + spare ❖ RAID 10
File Sharing Protocols	❖ CIFS/SMB ❖ NFS
Access Control	❖ Users have read-only or read/write access to shared folders ❖ CIFS users access shared folders using passwords

10. Understanding RAID and Storage Policies

Your LaCie Ethernet Disk RAID supports several different RAID levels: 0, 1, 5, 5+spare, and 10 (1+0). This section will help you decide which RAID level is right for your application.

RAID levels effect the total available storage capacity of the disks in the RAID array. The table below describes how each RAID levels affect the total storage capacity.

RAID Level	Available Capacity	Page
RAID 0	100%	Page 118
RAID 1	50%	Page 119
RAID 5	75%	Page 120
RAID 5+spare	50%	Page 121
RAID 10 (1+0)	50%	Page 122

10.1. RAID 0

Striped Disk Array Without Fault Tolerance

Also called striping, this level offers high transfer rates and is ideal for large blocks of data where speed is of the utmost importance.

RAID 0 implements a striped disk array, where all of the hard disks are linked together to form one large aggregate hard disk (Fig. 7.1.A.). In this configuration, data is broken down into blocks and each block is written to a separate disk drive within the array; I/O performance is greatly improved by spreading the I/O load across several drives. In this array, however, when one disk fails, all of the data on the array is lost.

Storage capacity is determined by the smallest disk in the array, and the smallest disk's capacity is applied to all of the other disks in the array. So, for instance, if you had four disks installed, ranging in capacity from 40GB to 80GB, when the RAID 0 array is built your system will see one, 160GB (40GB x 4) hard disk.

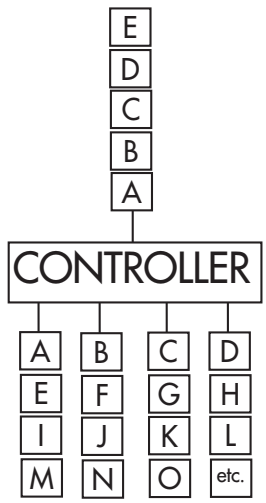
While this is a very simple and easily implemented design, RAID 0 should never be used in mission critical environments. When even just one disk in the array fails, all of the data on the entire array will be lost.

Recommended Uses

- Video production and editing
- Image editing
- Pre-press applications
- Applications requiring high-bandwidth

Characteristics and Advantages

- Data is broken down into blocks and each block is written to a separate disk drive
- I/O performance improved by spreading the load across multiple drives
- Overhead is lowered due to no calculations for parity
- Simple design and easily implemented



This diagram represents a RAID 0 array, consisting of four disks, which are connected to the Controller. Data blocks are distributed across all of the disks in the array.

Fig. 10.1.

10.2. RAID 1

Mirroring and Duplexing

Also called mirroring, this level makes a duplicate write on a second or "mirror" disk every time data is written to a primary disk. If one disk crashes, there is an ideal backup (Fig. 7.2.A.).

Using two controllers, or duplexing, can speed the data I/O rate by writing to both drives at the same time. When using just a single controller operations are slowed because data is written first to the data drive and then to the mirrored drive.

The storage capacity of a two-disk RAID 1 array is equal to the storage capacity of a single disk because the same data is duplicated on both disks. However, the 100 percent redundancy of data does not require a rebuild in the case of a drive failure. In that case, data can be copied to a replacement disk.

Characteristics and Advantages

- Can sustain multiple simultaneous drive failures in most cases
- Simplest RAID storage subsystem design
- Transfer rate for each block is the same as that of a single disk
- Data is 100 percent redundant

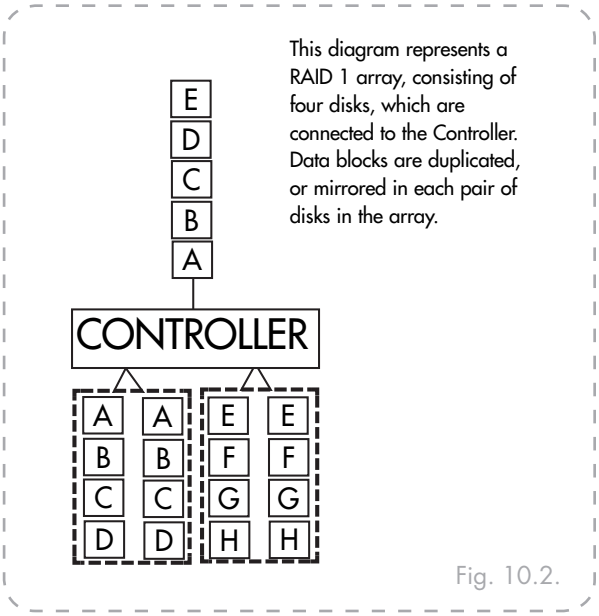


Fig. 10.2.

Recommended Uses

- Payroll
- Accounting
- Financial
- Any use that requires high availability

10.3. RAID 5

Data Striping with Striped Parity

Like RAID 0, RAID 5 offers increased performance by distributing the data across multiple disks. But unlike RAID 0, RAID 5 also offers data protection. If your Ethernet Disk RAID has three disks of equal size, two thirds of each disk are used for data, and the remaining third contains the parity information needed to reconstruct either of the other two. In this way, if any of the three disks fails, it can be reconstructed when a new disk is installed in the Ethernet Disk RAID.

If your Ethernet Disk RAID has four disks of equal size, three fourths of each disk are used for data, and the remaining fourth contains the parity information needed to reconstruct either of the other three. If any of the four disks fails, it can be reconstructed when a new disk is installed.

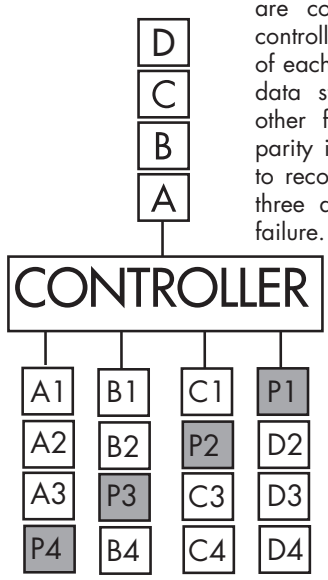
You can use RAID 5 only if your Ethernet Disk RAID has at least three disks. If the disks are not the same size, the smallest of the disks determines how much disk space is available for data. For example, if one disk is 300 GB, one is 400 GB, and one is 500 GB, only 300 GB from each disk can be used. Two thirds of each disk (200 GB) is used for storage space, and the remaining third is used for parity information. As a result, only 600 GB of disk space would be available for data.

Recommended Uses

- File and Application Servers
- Database Servers
- Web, E-mail and News Servers
- Intranet Servers

Characteristics and Advantages

- Highest Read data transaction rate
- Medium Write data transaction rate
- High efficiency through a low ratio of ECC (Parity) disks to data
- Good aggregate transfer rate



This diagram represents a RAID 5 array consisting of four disks, which are connected to the controller. Three-fourths of each disk is used for data storage and the other fourth holds the parity information used to reconstruct the other three disks in case of failure.

Fig. 10.3.

10.4. RAID 5 + Spare

In a RAID 5 + spare configuration, three of the disks use RAID 5, and the fourth is empty. If any of the three disks fails, it is immediately rebuilt using the fourth spare disk. As a result, you can remove the failed disk and still have the ongoing fast performance and data protection offered by RAID 5. When the failed disk is repaired or replaced and re-installed into the Ethernet Disk RAID, it automatically becomes the spare for the other functioning three.

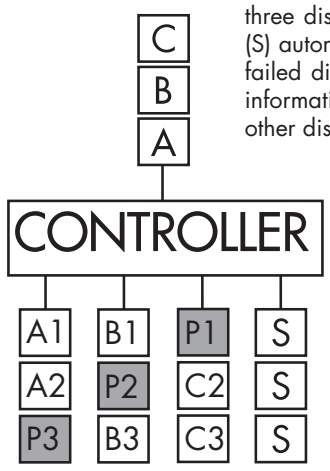
You can use RAID 5 + spare only if your Ethernet Disk RAID has four disks. If the disks are not the same size, the smallest of the disks determines how much disk space is available for data, similar to RAID 5.

Recommended Uses

- File and Application Servers
- Database Servers
- Web, E-mail and News Servers
- Intranet Servers

Characteristics and Advantages

- Highest Read data transaction rate
- Medium Write data transaction rate
- High efficiency through a low ratio of ECC (Parity) disks to data
- Good aggregate transfer rate



This diagram represents a RAID 5 array consisting of three disks. The fourth disk (S) automatically rebuilds a failed disk using the parity information stored on the other disks.

Fig. 10.4.

10.5. RAID 10 (RAID 1 + 0)

RAID 10 is similar to RAID 1, but rather than having one disk mirror to one other disk, two disks mirror to the two other disks.

You can use RAID 10 only if your Ethernet Disk RAID has four disks. The disks in the first two slots constitute the first pair, and the disks in the second two slots constitute the second pair. In each pair, the smaller of the two disks is used for data, and the larger of the two disks is used as the mirror.

If one disk in the pair fails, the other disk continues to make its data available.

Characteristics and Advantages

- Excellent data safety; three drives can fail without damaging data.
- Fast write speeds
- God for systems requiring high performance and fault tolerance

This diagram represents a RAID 10 array. Data is striped on two disks and those disks are mirrored by the other two.

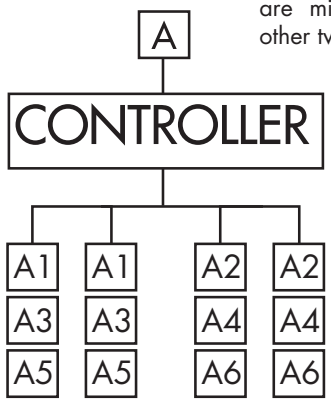


Fig. 10.5.

11. Contacting Customer Support

Before You Contact Technical Support

Read the User Manual and review the Troubleshooting section.

1. Try to isolate the problem. If possible, make the drive the only external device on the CPU, and make sure that all of the cables are correctly and firmly attached.

If you have asked yourself all of the pertinent questions in the troubleshooting checklist, and you still can't get your LaCie drive to work properly, contact us via the contacts in chapter 12.1 Bef ore contacting us, make sure that you are in front of your computer and that you have the following information on hand:

- Your LaCie drive's serial number
- Operating system and version
- Computer brand and model
- Amount of memory installed
- Names of any other devices installed on your computer, including CD/DVD burners

Information to Include in Email Correspondence

Information	Where to Find Information
1. LaCie Ethernet Disk RAID serial number	Located on a sticker at the back of drive or on the original packaging
2. Macintosh/PC model	**Mac users:** Click on the Apple icon in the menu bar and select **About this Mac**. **Windows users:** Right click **My Computer** and select **Properties > General**.
3. Operating system version	
4. Processor speed	
5. Computer memory	
6. The brands and models of other internal and external peripherals installed on my computer	**Mac users:** Click on the Apple icon in the finder bar and select **About this Mac**. Select **More Info...** The **Apple System Profiler** will launch and will list your internal and external peripherals. **Windows users:** Right click **My Computer** and select **Properties > Hardware.**

11.1. LaCie Technical Support Contacts

LaCie Asia, Singapore, and Hong Kong Contact us at: http://www.lacie.com/asia/contact/	LaCie Australia Contact us at: http://www.lacie.com/au/contact/
LaCie Belgium Contact us at: http://www.lacie.com/be/contact/ (Français)	LaCie Canada Contact us at: http://www.lacie.com/caen/contact/ (English)
LaCie Denmark Contact us at: http://www.lacie.com/dk/contact	LaCie Finland Contact us at: http://www.lacie.com/fi/contact/
LaCie France Contact us at: http://www.lacie.com/fr/contact/	LaCie Germany Contact us at: http://www.lacie.com/de/contact/
LaCie Italy Contact us at: http://www.lacie.com/it/contact/	LaCie Japan Contact us at: http://www.lacie.com/jp/contact/
LaCie Netherlands Contact us at: http://www.lacie.com/nl/contact/	LaCie Norway Contact us at: http://www.lacie.com/no/contact/
LaCie Spain Contact us at: http://www.lacie.com/es/contact/	LaCie Sweden Contact us at: http://www.lacie.com/se/contact
LaCie Switzerland Contact us at: http://www.lacie.com/chfr/contact/ (Français)	LaCie United Kingdom Contact us at: http://www.lacie.com/uk/support/request/
LaCie Ireland Contact us at: http://www.lacie.com/ie/contact/	LaCie USA Contact us at: http://www.lacie.com/contact/
LaCie International Contact us at: http://www.lacie.com/intl/contact/	

12. Warranty Information

LaCie warrants your drive against any defect in material and workmanship, under normal use, for the period designated on your warranty certificate. In the event this product is found to be defective within the warranty period, LaCie will, at its option, repair or replace the defective drive. This warranty is void if:

- The drive was operated/stored in abnormal use or maintenance conditions;
- The drive is repaired, modified or altered, unless such repair, modification or alteration is expressly authorized in writing by LaCie;
- The drive was subjected to abuse, neglect, lightning strike, electrical fault, improper packaging or accident;
- The drive was installed improperly;
- The serial number of the drive is defaced or missing;
- The broken part is a replacement part such as a pick-up tray, etc.
- The tamper seal on the drive casing is broken.

LaCie and its suppliers accept no liability for any loss of data during the use of this device, or for any of the problems caused as a result.

LaCie will not, under any circumstances, be liable for direct, special or consequential damages such as, but not limited to, damage or loss of property or equipment, loss of profits or revenues, cost of replacement goods, or expense or inconvenience caused by service interruptions.

Any loss, corruption or destruction of data while using a LaCie drive is the sole responsibility of the user, and under no circumstances will LaCie be held liable for the recovery or restoration of this data.

Under no circumstances will any person be entitled to any sum greater than the purchase price paid for the drive.

To obtain warranty service, call LaCie Technical Support. You will be asked to provide your LaCie product's serial number, and you may be asked to furnish proof of purchase to confirm that the drive is still under warranty.

All drives returned to LaCie must be securely packaged in their original box and shipped with postage prepaid.

IMPORTANT INFO: Register online for free technical support: www.lacie.com/register

Glossary

backup view – A backup that has been assigned a drive letter and can be opened and explored using My Computer or Windows Explorer

Console – The Windows-based application that enables you to discover all the storage systems on your subnet, view their version and network information, access the Manager, and map drive letters to shared folders

data disk or partition – A hard disk or partition of a hard disk that is not used to run the computer operating system

group – A collection of one or more users that can be given access to a shared folder all at once

jumbo frame – A large packet size for transferring data between an Ethernet Disk RAID and computers in the network

Manager – The Web-based user interface that enables you to configure the Ethernet Disk RAID

NIC – An acronym for network interface card

NTP – An acronym for Network Time Protocol, a mechanism for synchronizing a computer's

time with a standard time on a server

RAID – An acronym for redundant array of independent disks Different levels of RAID provide different types of data protection and data duplication, as well as enhance the performance of your disks.

remote boot – The process of booting your computer from the Ethernet Disk RAID rather than from a local hard disk

shared folder – A folder on the Ethernet Disk RAID that can be accessed by authorized users

subnet – A portion of a local area network. Computers in a subnet typically have IP addresses that are the same except for the last three digits. For example, computers with IP addresses of 192.168.0.101, 192.168.0.102, and 192.168.0.103 would all belong to the same subnet.

system disk or partition – EA hard disk or partition of a hard disk from which the computer boots

user – An individual or computer that can access a shared folder on the Ethernet Disk RAID